PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

RUY CARLOS GOMES DINI

A INFLUÊNCIA DO CONTEXTO NO COMPORTAMENTO RESPONSÁVEL RELATIVO À SEGURANÇA DA INFORMAÇÃO

Porto Alegre
Agosto de 2014

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

RUY CARLOS GOMES DINI

A INFLUÊNCIA DO CONTEXTO NO COMPORTAMENTO RESPONSÁVEL RELATIVO À SEGURANÇA DA INFORMAÇÃO

Porto Alegre
Agosto de 2014

RUY CARLOS GOMES DINI

A INFLUÊNCIA DO CONTEXTO NO COMPORTAMENTO RESPONSÁVEL RELATIVO À SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Administração e Negócios pelo Programa de Pós-Graduação em Administração da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul. (MAN/FACE/PUCRS).

Professora Orientadora: Profª Drª. Edimara Mezzomo Luciano

Porto Alegre

Agosto de 2014

D585i Dini, Ruy Carlos Gomes.
A influência do contexto no comportamento responsável relativo à segurança da informação. / Ruy Carlos Gomes Dini. – Porto Alegre, 2014.
155 f.

Dissertação (Mestrado em Administração e Negócios) – Programa de Pós Graduação em Administração, Faculdade de Administração, Contabilidade e Economia, PUCRS.
Orientador: Profª. Drª. Edimara Mezzomo Luciano

1. Administração de Empresas. 2. Segurança da Informação. 3. Comportamento Responsável. 4. Influência do Contexto. 5. Vulnerabilidade. I. Luciano, Edimara Mezzomo. II. Título.

CDD 658.4038

Ficha elaborada pela bibliotecária Anamaria Ferreira CRB 10/1494

Ruy Carlos Gomes Dini

A influência do Contexto no Comportamento Responsável Relativo à Segurança da Informação

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Mestrado em Administração e Negócios da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Aprovado em 27 de março de 2014, pela Banca Examinadora.

BANCA EXAMINADORA:

Profa. Dra. Edimara Mezzomo Luciano
Orientadora e Presidente da sessão

Profa. Dra. Marie Anne Macadar Moron

Prof. Dr. Maurício Gregianin Testa

Prof. Dr. Antonio Carlos Gastaud Maçada

Dedico este trabalho às minhas avós Eva Dini
e Ondina Gomes, que sempre batalharam
e me apoiaram em todos os momentos.

AGRADECIMENTOS

Inicialmente, gostaria de agradecer aos meus pais, João Carlos e Rosângela, que sempre me ofereceram o melhor, dentro do possível, e fizeram de mim a pessoa que sou hoje. Sempre levarei comigo seus ensinamentos. Apesar de não saber demonstrar isso muito bem, não tenho palavras para expressar meu amor por vocês. Muito Obrigado!

Gostaria de agradecer também a todos os meus amigos, que entenderam minha ausência nesses últimos tempos. Saibam que não me esqueci de nenhum de vocês. E nunca me esquecerei, sempre levo um pouco de cada um de vocês comigo. Como agradecimento especial, não posso deixar de lembrar de meu amigo Fábio Nunes, amigo desde os tempos do segundo grau, de meu amigo Miguel Nunez, amigo desde o curso técnico lá no Parobé e dos amigos de longa data Daniel Bender, Jefferson Renz e Luis Ricardo Gutierres, parcerias no futebol e no vídeo game. Todos grandes camaradas.

Também deixo meus agradecimentos aos amigos Vanessa Daniel, Bruno Fulginiti, Gabriela Viale, Eduardo Kunzel, Eduardo Codevilla, Felipe Nodari, Maurício Folli, Josiane Porto, Cristiano Kaehler, Mauren Soares, Alexandre Bampi, Marcelo Curth, Wladimir Pardo, Tatiana Rigobello, Ana Carla Palhares, Márcia Cezere, Guilherme Marra e Guilherme Wiedenhoft que participaram junto comigo nessa empreitada que foi cursar o mestrado.

Deixo agradecimentos especiais para minha professora orientadora Edimara Luciano. Agradeço mesmo por toda a sua compreensão diante da minha falta de tempo e por todos os conselhos nessa caminhada. Cresci muito com sua experiência. Muito obrigado!

Agradeço também aos componentes da minha banca, os professores Antonio Carlos Maçada, Marie Anne Moron e Maurício Testa, por todas as considerações feitas para aprimorar meu trabalho. E pela minha aprovação também!

Finalizo meus agradecimentos lembrando outros professores importantes nessa trilha, entre eles Aurora Zen, Cláudio Damacena e Leonardo de Oliveira. Eles motivam nossa busca pelo conhecimento. Agradeço também a secretária do MAN, Janaina Marques, pela atenção e pela presteza habituais, e aos amigos Felipe Baranzano e Bruna Martins, no auxílio das transcrições e análises. É importante lembrar e agradecer também aqueles que me motivaram e me apoiaram desde o início desse caminho, meus amigos professores Golber Royes e André Bender.

Enfim, agradeço a todos que de alguma forma me ajudaram nessa jornada.

Olhando para trás agora, vendo tudo que passou, não imaginava chegar aonde cheguei.

E talvez não chegasse se não fosse o apoio de todos vocês!

“Não há vitória sem persistência...”

Ruy Carlos Gomes Dini

RESUMO

Os incidentes internos de Segurança da Informação ainda continuam sendo considerados os mais presentes na realidade organizacional atual. Apesar de estudos anteriores ressaltarem a importância dos aspectos humanos ou comportamentais na gestão de Segurança da Informação, normalmente eles são deixados em segundo plano pelas organizações. No entanto, o comportamento do colaborador pode ser o elemento mais significativo no cumprimento e na aplicação de uma Política de Segurança da Informação, visto que diversos fatores presentes no contexto em que os funcionários estão inseridos podem influenciar nesse comportamento. A partir de um modelo conceitual desenvolvido com base em estudos anteriores, um roteiro de entrevistas foi elaborado, testado, validado e aplicado em 14 entrevistas com CIOs ou gestores de cargo equivalente de grandes empresas que utilizam práticas e esforços diários para manter a Segurança da Informação. Com a interpretação das entrevistas realizadas, foi possível identificar a influência percebida de fatores do contexto organizacional e do contexto de Tecnologia e Segurança da Informação no comportamento responsável dos funcionários relativo à Segurança da Informação, na intenção de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação. Os resultados apontam fortes indícios da relação do contexto organizacional no comportamento responsável, pois todas as variáveis estudadas foram percebidas pelos entrevistados. Em relação ao contexto de Tecnologia e Segurança da Informação, a maioria das variáveis obteve influência percebida no comportamento responsável. Com base na análise de conteúdo categorial das entrevistas, também foi possível identificar os fatores desencadeadores do comportamento responsável relacionado à Segurança da Informação, que traz implicações positivas na efetividade da gestão de Segurança da Informação das organizações.

Palavras-chave: Segurança da Informação. Comportamento Responsável. Influências do Contexto. Vulnerabilidade a Ameaças Internas de Segurança da Informação

ABSTRACT

Internal Information Security incidents are still considered as the most present in the current organizational reality. Although previous studies have emphasized the importance of human and behavioral aspects in the management of Information Security, they are usually left in the background by organizations. However, the behavior of the employee may be the most significant element in the compliance and implementation of an Information Security Policy, since several factors present in the context in which employees are embedded can influence this behavior. From a conceptual model developed based on previous studies, an interviews script was developed, tested, validated and applied in 14 interviews with CIOs or equivalent managers of large companies that use practices and daily efforts to maintain the Information Security. With the interpretation of the interviews, it was possible to identify the perceived influence of factors of the organizational context and the context of Technology and Information Security in the responsible employee behavior on Information Security, in an attempt to protect against the insider threat vulnerabilities of information security. The results show strong evidence of the relationship of the organizational context on responsible behavior, because all variables were perceived by respondents. In relation to the context of Technology and Information Security, most of the variables obtained in the perceived influence responsible behavior. Based on the categorical content analysis of the interviews, it was also possible to identify the triggers of responsible behavior related to Information Security, which has positive implications for the effectiveness of managing information security in organizations.

Keywords: Information Security. Responsible Behavior. Influences of Context. Insider Threat Vulnerabilities of Information Security.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Este capítulo tem o objetivo de definir o escopo deste estudo, destacando a importância do tema principal do trabalho, Segurança da Informação, com foco específico na relação de influência dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável visando evitar vulnerabilidades a ameaças internas de Segurança da Informação. A abordagem do tema apresentado neste estudo é diferente das pesquisas científicas tradicionalmente realizadas na área, que focam em aspectos técnicos ou acerca de políticas de Segurança da Informação especificamente, pois contempla fatores comportamentais relacionados à Segurança da Informação. Este trabalho foca nos contextos organizacional e de Tecnologia e Segurança da Informação que influenciam os indivíduos, basicamente funcionários ou colaboradores das empresas, a se comportarem de maneira responsável em relação à Segurança da Informação, ou seja, de acordo com as regras e normas da política de Segurança da Informação, no sentido de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação. Conforme a definição do tema, do foco e do problema de pesquisa, são apresentadas a questão de pesquisa, bem como os objetivos, geral e específicos, e a justificativa deste estudo. Além destes itens citados, este tópico é finalizado com a estrutura completa da dissertação.

1.1 TEMA E FOCO DA PESQUISA

Numa época onde a informação é um elemento fundamental para a sobrevivência das organizações, a Segurança da Informação desempenha a importante função de proteger os ativos informacionais de uma organização. As organizações têm focado principalmente em soluções técnicas para prevenir ataques ou incidentes de Segurança e poucas utilizam uma abordagem sócio-técnica que possa tratar aspectos não-técnicos em relação à Segurança da Informação (DHILLON e BACKHOUSE, 2001).

Observa-se que somente aspectos técnicos de Segurança da Informação não são capazes de garantir um ambiente relativamente seguro (ROTVOLD, 2008; HERATH e RAO, 2009b), e se as organizações não considerarem a Segurança da Informação sob todos os ângulos possíveis, elas provavelmente estarão vulneráveis. A importância de aspectos não-técnicos de Segurança da Informação está na possibilidade deles permitirem enfocar outros aspectos também relevantes neste contexto, tais como fatores organizacionais, culturais e individuais que podem influenciar na vulnerabilidade da Segurança da Informação das

organizações e podem auxiliar gestores e estudiosos no entendimento da realidade atual vivenciada nas empresas.

Os indivíduos, considerados a parte principal de todo o processo de Segurança da Informação, são responsáveis pelo gerenciamento da informação e podem ter acesso a diversos níveis de informações confidenciais (ROTVOLD, 2008). Porém, as pessoas também são a parte mais suscetível a erros e degradações, pois os aspectos individuais variam de acordo com cada pessoa e com o ambiente no qual ela está inserida (VAAST, 2007). É importante salientar que não há garantias de que uma organização com políticas e práticas de Segurança da Informação bem definidas tenha plena aderência e conscientização dos funcionários em relação a práticas e procedimentos de segurança desejados (HERATH e RAO, 2009b).

Outro aspecto a considerar é o contexto organizacional, que afeta os empregados de maneira com que a satisfação com o ambiente influencie no comportamento individual relativo à Segurança da Informação (CHAN, WOON e KANKANHALLI, 2005), o que pode implicar, em caso de aparente baixa satisfação, pouco comprometimento do funcionário no atendimento às políticas, práticas e controles de Segurança da Informação e, consequentemente, chances de causar sérios riscos com o aumento de vulnerabilidades no ambiente de Tecnologia da Informação. Condições de trabalho desfavoráveis, tais como pressão por tempo ou metas e temperamento instável dos supervisores, de acordo com Vroom e Von Solms (2004), e falta de reconhecimento profissional, salário incompatível com a função exercida e stress no ambiente de trabalho, segundo Luciano, Mahmood e Maçada (2010), podem ser a causa de uma baixa motivação do colaborador, originando implicações negativas para a gestão de Segurança da Informação de toda uma organização. Seguindo essa mesma visão, Albrechtsen (2007) verificou que um grande volume de trabalho para garantir um ambiente de Tecnologia da Informação seguro cria conflitos de prioridade entre utilidade, eficiência e funcionalidade dos processos organizacionais, o que também indica possíveis problemas relacionados com os fatores organizacionais na gestão de Segurança da Informação.

Assim, diante do contexto organizacional que, consequentemente, pode influenciar no comportamento relacionado com Segurança da Informação, nota-se que o comportamento dos colaboradores pode variar conforme a percepção que os empregados têm do ambiente organizacional de maneira geral, segundo Wulff, Bergman e Sverke (2009), e quanto às condições de trabalho oferecidas pela empresa, de acordo com Dulebohn *et al*. (2009). Logo, pode-se sugerir que o contexto de Tecnologia e Segurança da Informação, bem como o

entendimento intrínseco sobre Tecnologia da Informação e Segurança da Informação (LACEY, 2009), além dos mecanismos de controles compreendidos (D'ARCY, HOVAV e GALLETTA, 2008) e das medidas punitivas previstas na política de Segurança (HERATH e RAO, 2009a), também afetam o comportamento individual de um funcionário relacionado à Segurança da Informação.

Kwantes e Boglarsky (2007), em uma pesquisa realizada em seis países, observaram que a cultura organizacional tem efeito sobre o desempenho individual de cada pessoa. Logo, a cultura da organização também pode ter relação com o comportamento dos empregados relativo à Segurança da Informação. A cultura organizacional diz respeito às ideias compartilhadas e difundidas entre os indivíduos presentes na empresa, considerando os artefatos, os valores expostos e as suposições tácitas ou crenças compartilhadas (VROOM e VON SOLMS, 2004). Desta forma, fatores culturais da organização podem afetar os seus membros e a própria organização em si. Os gestores da organização podem adotar abordagens para moldar a cultura e promover um ambiente propício para o sucesso de iniciativas de Segurança da Informação (CHANG e LIN, 2007). Desenvolver o conhecimento em Segurança da Informação dos funcionários, criar políticas de Segurança de acordo com as necessidades da organização e conscientizar colaboradores quando uma determinada crença individual entrar em conflito com valores adotados pela empresa, tais como políticas, praticas e controles de Segurança, são aspectos a serem avaliados no desenvolvimento de uma cultura favorável à Segurança da Informação (VAN NIEKERK e VON SOLMS, 2010).

Tanto aspectos organizacionais quanto culturais convergem para o comportamento individual de um colaborador. Logo, verifica-se que aspectos individuais estão diretamente relacionados com a vulnerabilidade a ameaças internas de Segurança da Informação, já que o comportamento do empregado poderá influenciar no cumprimento das políticas, práticas e controles de Segurança da Informação. Aspectos que implicam no comportamento responsável relacionado à Segurança da Informação compreendem a capacitação dos funcionários com o objetivo de fornecer conhecimento por parte de políticas, práticas e controles em relação à Segurança da Informação (RANSBOTHAM e MITRA, 2009), conscientização sobre os possíveis danos à empresa (KRUGER e KEARNEY, 2006) e o comportamento adequado a ser desempenhado, através de programas de treinamento (D'ARCY, HOVAY e GALLETTA, 2009). Alguns autores também incluem variações no comportamento de usuários de Tecnologia da Informação de acordo com o gênero dos funcionários (VENKATESH *et al*., 2003), a experiência adquirida no desempenho de seu trabalho e a lealdade dos colaboradores perante a empresa (LACEY, 2009; LUCIANO,

MAHMOOD e MAÇADA, 2010), os quais também podem ser considerados aspectos individuais relevantes e com capacidade significativa de potencializar vulnerabilidades a ameaças internas de Segurança da Informação nas organizações.

Assim sendo, o contexto organizacional e de Tecnologia e Segurança da Informação observado pelo ponto de vista dos funcionários, incluindo as condições de trabalho oferecidas pela organização, a cultura da organização e sua relação com a Segurança da Informação, o comportamento dos funcionários relacionado às políticas, práticas e controles de Segurança da Informação, a familiaridade dos funcionários com as políticas, práticas e controles de Segurança da Informação, a conscientização dos colaboradores em relação às principais ameaças de Segurança da Informação para a organização, entre outros motivos, são aspectos não-técnicos de extrema importância para garantir a Segurança da Informação em uma organização (LUCIANO, MAHMOOD e MAÇADA, 2010). Neste ponto encontra-se o foco desta pesquisa, que busca investigar a influência dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável dos funcionários das organizações relacionado à Segurança da Informação, a fim de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação.

1.2 PROBLEMA DE PESQUISA

A partir da década de 80, a Tecnologia da Informação adquiriu funções estratégicas mais complexas nas organizações, funções estas que incluem desde o apoio às atividades vitais da empresa, tais como minimização de riscos e redução de custos ou até como forma de buscar vantagens competitivas de acordo com a maneira com que ela é utilizada (HENDERSON e VENKATRAMAN, 1993). Assim, a informação passou a ser considerada de grande importância por possuir alta capacidade de agregar valor aos processos, serviços e produtos, sendo um fator crítico para atingir os objetivos principais de qualquer organização (BEAL, 2005). Com o avanço tecnológico proporcionado desde sua invenção, a Tecnologia da Informação transformou o mundo empresarial, trazendo consigo melhoras significativas na produtividade dos negócios, mas também vários problemas para a Segurança da Informação (LACEY, 2009). A confiança das organizações em utilizar Sistemas de Informação para a transmissão, processamento e armazenamento da informação aumentou, o que também acarretou em uma maior necessidade de investimentos e melhores práticas de Segurança da Informação (NG, KANKANHALLI e XU, 2009).

Diante dessa situação, surge então a preocupação com a Segurança da Informação, que tem como objetivo principal fornecer proteção aos ativos informacionais de uma organização relativo a perdas, exposição indevida ou dano (WILLIAMS, 2001), com a finalidade de manter o empreendimento, diminuir perdas empresariais e maximizar o retorno dos investimentos e as oportunidades de negócios (MANDARINI, 2004). Em virtude dos danos causados por inúmeros incidentes de Segurança da Informação (NG, KANKANHALLI e XU, 2009), confirmados por Peters (2009), que observou aumentos significativos na incidência de diversos ataques a Sistemas de Informação com perdas financeiras relativamente altas nos Estados Unidos em 2009, e pela PwC Brasil (2012), que identificou os crimes digitais como o segundo principal crime econômico contra empresas no Brasil em 2011, as organizações buscaram maior investimento em soluções tecnológicas e mecanismos de proteção da informação (NG, KANKANHALLI e XU, 2009; TRCEK *et al*., 2007).

No entanto, a Segurança da Informação não abrange somente aspectos técnicos, mas atinge também aspectos individuais e comportamentais das pessoas, e assim se faz necessária uma abordagem de gestão que leve em consideração a cultura, a educação, o conhecimento e, principalmente, a conscientização dos indivíduos acerca dos meios corretos e seguros para usar as ferramentas de TI, conforme a visão de Luciano, Mahmood e Maçada (2010). De acordo com Dutta e Roy (2008), aspectos individuais devem ser considerados na manutenção da Segurança da Informação, pois muitas ameaças são ocasionadas por usuários ou funcionários (ALDER, NOEL e AMBROSE, 2006), tanto por motivos acidentais ou intencionais (RANSBOTHAM e MITRA, 2009), podendo ser provocadas pelo contexto organizacional em que os indivíduos estão inseridos (WILLIAMS, 2001). Além disso, somente soluções técnicas de Tecnologia da Informação não são suficientes para garantir a proteção dos ativos de informação, pois a efetividade da Segurança da Informação depende justamente do comportamento de cada indivíduo e a conduta inadequada do colaborador pode originar inúmeras vulnerabilidades a ameaças internas de Segurança da Informação. Pesquisas realizadas por Cho (2006), Son e Kim (2008) e Coronado *et al*. (2009) confirmam a utilidade latente de conceitos de vulnerabilidade, risco, confiança e privacidade na área de Segurança da Informação.

Como nenhum Sistema de Informação é totalmente seguro (STRAUB e WELKE, 1998), atentar para os aspectos individuais envolvidos na Segurança da Informação pode auxiliar no entendimento desse fenômeno, conforme os estudos de Ng, Kankanhalli e Xu (2009) e de Liginal, Sim e Khansa (2009) sobre aspectos individuais, e os trabalhos de Dhillon e Backhouse (2001) e de Dourish e Anderson (2006) sobre aspectos sociais. Num

ambiente de relativa complexidade, manter a Tecnologia da Informação segura necessita uma compreensão que vá além de aspectos técnicos, segundo Luciano, Mahmood e Maçada (2010).

Todo o contexto organizacional pode impactar na vulnerabilidade a ameaças internas de Segurança da Informação de forma que o indivíduo tenha um comportamento inadequado a partir das percepções que ele tem do clima organizacional e das condições de trabalho oferecidas pela empresa. O clima organizacional insatisfatório e condições de trabalho desfavoráveis podem contribuir para a falta de motivação do colaborador em manter-se de acordo com políticas, práticas e controles de Segurança, o que representa um sério fator de risco, a ponto de fazer com que as vulnerabilidades a ameaças internas de Segurança da Informação sejam inevitáveis.

Incluída no contexto organizacional, a cultura organizacional também pode afetar o comportamento do indivíduo enquanto funcionário de uma organização que, dependendo da situação, pode acarretar em vulnerabilidades a ameaças internas de Segurança da Informação. Hofstede, Hofstede e Minkov (2010) definem cultura organizacional como um fenômeno coletivo, compartilhado em parte com indivíduos que pertencem ou pertenceram a um determinado contexto social onde a cultura foi aprendida, diferenciando esse grupo de indivíduos de outros grupos. Culturas organizacionais com valores, hábitos ou crenças que favoreçam a competição entre colaboradores ou que não consideram a Segurança da Informação na proteção de seus ativos informacionais poderão contribuir para um comportamento individualista dos funcionários, fazendo com que a Segurança da Informação seja negligenciada e permita o surgimento de vulnerabilidades que poderão ser exploradas mais facilmente.

Fatores relacionados com o contexto de Tecnologia e Segurança da Informação também pressupõem relação direta no comportamento dos empregados acerca de Segurança da Informação. O conhecimento e a experiência em relação à Tecnologia da Informação (WORKMAN, BOMMER e STRAUB, 2008), o conhecimento e a severidade da política de Segurança da Informação (LEE, LEE e YOO, 2004) e os mecanismos de controle, monitoramento e possíveis punições aplicáveis (HERATH e RAO, 2009a) podem ser considerados parte integrante na formação do comportamento individual de acordo com a percepção de cada funcionário, o que pode ocasionar erros e/ou omissões na Segurança da Informação, provocando possíveis vulnerabilidades a ameaças internas.

De acordo com os dois contextos apresentados anteriormente, observa-se então que ambos estão diretamente relacionados com o comportamento responsável em relação à

Segurança da Informação. Assim, todo o comportamento individual de Segurança da Informação será impactado pelos aspectos contextualizados de uma organização. Se uma organização não fornece treinamento e conhecimento de Segurança da Informação e não conscientiza seus colaboradores sobre os perigos e ameaças à vulnerabilidade dos Sistemas de Informação da organização, é possível que o comportamento apresentado pelos empregados esteja sujeito a falhas que possibilitem incidentes de Segurança da Informação. Da mesma forma, culturas organizacionais que não valorizam a Segurança da Informação possivelmente ocasionarão comportamentos pouco responsáveis e preocupados com a segurança de ativos da organização. Adotar uma perspectiva holística de Segurança da Informação nas quais questões humanas, organizacionais e técnicas têm igual importância é a melhor alternativa para explicar os fatores que influenciam o comportamento e a conscientização relacionada à Segurança da Informação, principalmente se esses estudos forem em países em desenvolvimento (REZGUI e MARKS, 2008).

Segundo essa perspectiva, nota-se que o tema de pesquisa está relacionado principalmente a aspectos não-técnicos de Segurança da Informação, com foco nos contextos organizacional e de Tecnologia e Segurança da Informação e suas influências no comportamento responsável a fim de evitar vulnerabilidades a ameaças internas de Segurança da Informação. Partindo desse pressuposto, apresenta-se a questão de pesquisa que esse trabalho busca responder: **Qual a relação de influência dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável dos colaboradores visando evitar vulnerabilidades a ameaças internas de Segurança da Informação?**

1.3 OBJETIVOS

Nesta seção, são apresentados os objetivos geral e específicos que compõem o presente estudo com a finalidade de sintetizar as ideias apresentadas no tópico de tema e foco da pesquisa, bem como nortear o sentido da pesquisa de acordo com o situação problemática proposta.

1.3.1 Objetivo geral

Identificar a relação de influência dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável dos funcionários visando evitar

vulnerabilidades a ameaças internas de Segurança da Informação, a partir da percepção dos gestores de TI das organizações estudadas.

1.3.2 Objetivos específicos

Como forma de atingir o objetivo geral deste trabalho, são apresentados os seguintes objetivos específicos:

a) Identificar a presença ou não da relação de influência percebida do contexto de Tecnologia e Segurança da Informação no comportamento responsável dos colaboradores relativo à Segurança da Informação;

b) Identificar a presença ou não da relação de influência percebida do contexto organizacional no comportamento responsável dos funcionários relativo à Segurança da Informação;

c) Identificar a presença ou não da relação de influência percebida do comportamento responsável relativo à Segurança da Informação dos empregados na proteção contra vulnerabilidades a ameaças internas de Segurança da Informação;

d) Evidenciar fatores desencadeadores do comportamento responsável dos colaboradores relativo à Segurança da Informação na proteção contra vulnerabilidades a ameaças internas de Segurança da Informação.

1.4 JUSTIFICATIVA

A Segurança da Informação é uma área presente em qualquer tipo de organização atualmente. Conforme o avanço significativo das tecnologias, também surgiram diversas novas ameaças para os Sistemas de Informação, que aumentam mais a cada ano. Nos Estados Unidos, em uma comparação entre os anos de 2008 e 2009, houve significativos aumentos na incidência de fraudes financeiras (12% em 2008 e 19,5% em 2009), infecções de *malware* (50% em 2008 e 64,3% em 2009), negação de serviço (21% em 2008 e 29,2% em 2009) e invasões de sites da internet (6% em 2008 e 13,5% em 2009), conforme a *CSI Computer Crime and Security Survey* de 2009 (PETERS, 2009). Segundo o autor, se contabilizadas as perdas em fraudes financeiras que ocorreram em 2009, quase 450 mil dólares foram perdidos por cada organização norte-americana que sofreu esse tipo de ataque.

No Brasil, os crimes digitais foram considerados o segundo principal crime econômico contra as empresas em 2011 (PWC BRASIL, 2012), sendo que a fonte mais provável desses

incidentes de Segurança da Informação seja de origem interna, ou seja, provocados por seus próprios funcionários, os chamados *insiders* (PWC BRASIL, 2012; PWC INTERNATIONAL, 2011). Mesmo com um aumento recente no volume de ameaças externas no mundo (EY GLOBAL, 2013) e apesar do grande investimento das organizações em recursos tecnológicos e informacionais para proteção dos Sistemas de Informação e consequente minimização dos riscos relacionados à Segurança, o comportamento humano inadequado continua sendo a maior ameaça interna à Segurança da Informação (LACEY, 2010), pois basta um funcionário com más intenções ou com treinamento insuficiente para tornar um simples procedimento diário num incidente de Segurança de proporções catastróficas para a empresa.

Com uma frequência anual de uma brecha de Segurança por empresa ocasionada por violações na política de Segurança da Informação, observa-se que mais da metade dessas violações são originadas a partir de um erro durante a realização dos procedimentos de Segurança feitos por um funcionário (VANCE, SIPONEN e PAHNILA, 2012). Como consequências comerciais negativas dessas violações nas empresas do Brasil em 2011, o dano à reputação da organização foi considerado o mais preocupante, seguido da interrupção de serviços e depois pelas perdas financeiras (PWC BRASIL, 2012). No entanto, em 2013, os dados brasileiros relativos à consequência dos incidentes de Segurança da Informação apontam que as perdas financeiras foram em maior número, com as perdas de clientes e o comprometimento da marca ou da reputação na sequência, além da indisponibilidade temporária de suas operações em decorrência desses incidentes (PWC INTERNATIONAL, 2013).

Assim, observa-se que os prejuízos causados por uma exposição na Segurança da Informação estão cada vez mais altos (NG, KANKANHALLI e XU, 2009), o que também faz aumentar ainda mais a preocupação das empresas em relação à Segurança da Informação. Ainda que existam diversas formas de proteger os dados e as informações dentro do ambiente organizacional, nenhum Sistema de Informação é totalmente seguro (STRAUB e WELKE, 1998). Diversos aspectos como vulnerabilidade, confiança, lealdade, risco e efetividade, além dos aspectos técnicos, estão relacionados com a Segurança da Informação (CORONADO *et al*., 2009). Diante dessa complexa situação, aspectos organizacionais e individuais necessitam de uma melhor explicação no ambiente de Tecnologia e Segurança da Informação de uma organização.

Partindo do ponto em que todo e qualquer Sistema de Informação está relacionado, em algum momento ou de alguma forma, com pessoas, consideradas o “elo fraco” da Segurança

da Informação por apresentarem aspectos individuais que variam de pessoa a pessoa ou de acordo com o contexto em que ela está inserida (BEAL, 2005; VAAST, 2007), fica evidente que o comportamento individual dos colaboradores é de grande importância para garantir a segurança dos ativos de informação organizacionais e merecem maior atenção das pesquisas científicas. Pessoas são complexas e completamente diferentes, variando suas atitudes de acordo com as influências exercidas por fatores como idade, personalidade, estilo de vida, cultura e pressão por alcance de metas (LACEY, 2009). Segundo esse mesmo autor, o aspecto individual sempre será considerado o ponto fraco da Segurança da Informação, pois indivíduos estão longe de serem perfeitos, cometem erros e podem ser facilmente persuadidos, o que já representa um importante motivo para a compreensão das influências que afetam o comportamento individual relacionado às vulnerabilidades a ameaças internas de Segurança da Informação.

Como o comportamento do indivíduo está presente em todo e qualquer ambiente de Tecnologia da Informação, a Segurança da Informação também passa por sua responsabilidade (VROOM e VON SOLMS, 2004; TRCEK *et al*., 2007). Conforme Choden *et al*. (2009), a conscientização do colaborador relativo às políticas de Segurança da Informação, as atitudes do funcionário e a aderência contínua às políticas, práticas e controles são determinantes para o sucesso da gestão de Segurança da Informação, porém são objetivos difíceis de serem atingidos e mensurados. Assim, cabe ressaltar a importância de um estudo com uma abordagem comportamental sobre Segurança da Informação, já que o comportamento do colaborador é fator determinante no atendimento da política de Segurança (DA VEIGA e ELOFF, 2010).

Como forma de melhorar o impacto do comportamento humano na Segurança da Informação, a capacitação e a conscientização das principais ameaças são ferramentas muito utilizadas (D'ARCY, HOVAV e GALLETTA, 2009). No entanto, segundo esses autores, somente essas ferramentas não são suficientes para conseguir práticas adequadas de Segurança da Informação, pois existem aspectos comportamentais, psicológicos, sócio-culturais e emocionais envolvidos que influenciam os indivíduos de maneira única e exclusiva.

Para compreender plenamente os aspectos individuais que afetam a vulnerabilidade do ambiente de Tecnologia da Informação das organizações, é mister analisar os motivos que antecedem e influenciam o comportamento individual. Dessa forma, surge a necessidade do estudo sobre os contextos organizacional e de Tecnologia e Segurança da Informação que impactam no comportamento do usuário em relação à Segurança da Informação. Estudos

anteriores apontam que a satisfação com o ambiente organizacional, medida pelo clima organizacional, tem efeito sobre o comportamento do indivíduo em relação à Segurança da Informação (CHAN, WOON e KANKANHALLI, 2005), bem como as condições de trabalho julgadas inadequadas pelos empregados (VROOM e VON SOLMS, 2004; LUCIANO, MAHMOOD e MAÇADA, 2010).

A cultura organizacional, a partir dos artefatos, valores e crenças compartilhadas, tenta transmitir aos funcionários a maneira de agir (*modus operandi*) considerada pela empresa. Deste modo, a organização pode induzir o comportamento do usuário em relação às políticas, práticas e controles de Segurança da Informação (CHANG e LIN, 2007; VAN NIEKERK e VON SOLMS, 2010), o que ressalta a importância do estudo e sua relação com o comportamento individual.

Lacey (2009) concorda também que aspectos organizacionais e individuais, tais como gênero, experiência no trabalho, lealdade do empregado, cultura organizacional, ambiente organizacional e condições de trabalho, podem impactar os funcionários de forma diferenciada. Diante de toda a complexidade da situação, pode-se concluir que um ambiente de Tecnologia da Informação seguro depende necessariamente do comportamento efetivo dos usuários (NG, KANKANHALLI e XU, 2009), nesse caso, os colaboradores da organização. Logo, examinar e compreender quais fatores do contexto organizacional e do contexto de Tecnologia e Segurança da Informação afetam o comportamento responsável dos funcionários em relação à Segurança na tentativa de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação é de suma importância para um melhor aperfeiçoamento das práticas e procedimentos que garantem uma relativa Segurança dos ativos informacionais das organizações, facilitando o gerenciamento do fator mais crítico de todo o processo de Segurança da Informação, as pessoas.

1.5 ESTRUTURA DO TRABALHO

Esta dissertação está dividida em capítulos que contemplam a introdução ao tema de pesquisa, a fundamentação teórica essencial sobre o assunto em questão, o método de pesquisa utilizado, os resultados finais obtidos na realização desta e as considerações finais sobre o estudo, além das referências e dos apêndices. O primeiro capítulo compreende a definição do tema e do foco de pesquisa, bem como o problema, a questão de pesquisa e os objetivos, geral e específicos, baseados no problema exposto anteriormente e que buscarão responder a questão de pesquisa formulada. Em seguida, é apresentada a justificativa para a

escolha do tema de estudo, que é a influência dos contextos organizacionais e de Tecnologia e Segurança da Informação no comportamento responsável dos colaboradores em relação à Segurança da Informação no sentido de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação. Finalizando este capítulo, encontra-se a estrutura da dissertação aqui apresentada, procurando facilitar a leitura e o entendimento da relação entre os tópicos abordados.

No segundo capítulo encontra-se o embasamento teórico da pesquisa, abordando os principais assuntos referentes ao tema em questão: gestão e proteção da informação; Segurança da Informação; e vulnerabilidades a ameaças internas de Segurança da Informação. No entanto, a seção Segurança da Informação está subdividida em: aspectos organizacionais de Segurança da Informação e comportamento responsável relativo à Segurança da Informação. Neste capítulo também é exposto o modelo conceitual em que a pesquisa é baseada.

O capítulo três aborda o método de pesquisa utilizado na dissertação, relatando todo o delineamento metodológico, assim como a coleta e a análise dos dados utilizados no estudo. Em seguida, a quarta etapa apresenta os resultados alcançados a partir da análise dos dados da pesquisa. Logo depois, encontram-se as considerações finais do autor, assim como as contribuições, as limitações do estudo em questão e as sugestões para pesquisas futuras, o que finaliza o quinto e último capítulo. Concluindo o trabalho, estão as referências utilizadas na pesquisa, seguidas pelos apêndices.

2 VULNERABILIDADE EM SEGURANÇA DA INFORMAÇÃO

Neste capítulo são apresentados os conceitos necessários para o entendimento do presente estudo em relação à influência dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável dos funcionários relativo à Segurança da Informação a fim de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação. Entre as temáticas que serão destacadas no referencial teórico estão: gestão e proteção da informação; Segurança da Informação; e vulnerabilidades a ameaças internas de Segurança da Informação. Gestão e proteção da informação abordarão a relevância da informação estratégica para as organizações na era da informação, as formas existentes utilizadas para proteger as informações organizacionais, assim como mecanismos regulatórios e instrumentos disciplinadores usados no contexto atual. No tópico de Segurança da Informação, os aspectos organizacionais e individuais de Segurança da Informação serão abordados, destacando temas como confiança, conhecimento, familiaridade e comportamento responsável dos empregados ou usuários de Tecnologia da Informação, ambiente organizacional e condições de trabalho, além da lealdade, do gênero, da experiência dos funcionários. O tópico sobre vulnerabilidades a ameaças internas de Segurança da Informação abordará as fraquezas dos sistemas informacionais e as ameaças que podem explorar essas vulnerabilidades na Segurança dos Sistemas de Informação das organizações. Finalizando este capítulo, encontra-se o modelo conceitual proposto em que esta pesquisa estará inicialmente baseada.

2.1 GESTÃO E PROTEÇÃO DA INFORMAÇÃO

A informação é atualmente considerada um dos principais ativos de uma organização. Dada tamanha importância, juntamente com o aumento da complexidade do ambiente em que as organizações estão inseridas, foram necessárias a criação de ferramentas eficazes para a proteção da informação (BEAL, 2005). Quanto maior o avanço dos riscos que envolvem a informação, maiores são as fraquezas dos processos de proteção nas empresas (MANDARINI, 2004). O alto número de casos de fraudes contras as organizações demonstra a seriedade do caso (BEAL, 2005; RICHARDSON, 2008; PETERS, 2009).

Diante deste contexto, percebe-se que a informação desempenha um papel fundamental para as organizações em todos os sentidos. O ato de obter informações disponíveis oportunamente, de maneira segura, clara e precisa oferece um grande diferencial

estratégico para quem a obtém (BEAL, 2005). Segundo Sêmola (2003), a informação sempre esteve presente nas organizações, independentemente de seu ramo de atuação ou porte da empresa, visando melhor produtividade, competitividade e apoio à tomada de decisão. Os computadores e a internet somente transpuseram o acesso local da informação, tornando-a globalizada (SÊMOLA, 2003). Atualmente, a informação está presente tanto no contexto individual quanto no organizacional, com ênfase para a proteção e Segurança da Informação (MANDARINI, 2004). Sêmola (2003) afirma que existem quatro etapas em que a informação fica exposta a ameaças, onde a integridade, a disponibilidade e a confidencialidade, que são os fundamentos da Segurança da Informação, podem ser afetadas:

- Manuseio: Instante em que a informação é manipulada ou criada;
- Armazenamento: Etapa em que a informação é guardada ou armazenada;
- Transporte: Fase em que a informação é enviada ou transportada;
- Descarte: Momento em que a informação é inutilizada ou descartada.

Não importando a etapa deste ciclo em que a informação se encontra, ela sempre deve estar protegida e controlada (SÊMOLA, 2003).

A Segurança da Informação deve seguir um processo de implementação de uma série de controles que incluem políticas, práticas, procedimentos, estruturas organizacionais e funções de *software* e *hardware* (ABNT, 2005). Diante da importância da Tecnologia da Informação para as empresas, a Segurança da Informação se tornou a base principal para o gerenciamento das organizações modernas (CHANG e HO, 2006). Von Solms e Von Solms (2005) ressaltam que a Segurança da Informação é um tema complexo, relacionado ao negócio em geral, que necessita a identificação dos potenciais riscos, envolvimento dos funcionários, além de ferramentas e uma estrutura básica necessárias, considerada indispensável para as organizações atuais.

No entanto, a área da Segurança da Informação não consegue atender corretamente às expectativas em relação aos aspectos individuais e sócio-organizacionais (DHILLON e BACKHOUSE, 2001), já que muitos gestores negligenciam o comportamento individual nas relações de Segurança da Informação. Com o objetivo de buscar uma segurança plena e efetiva, medidas preventivas devem ser utilizadas, além do uso de mecanismos de punição para conter ataques contra a Segurança da Informação (SÊMOLA, 2003). Normas também foram criadas para estabelecer políticas de Segurança da Informação nas organizações, entre elas, a NBR ISO/IEC 17799 (substituída pela ISO/IEC 27002, que trata sobre as boas práticas de sistemas de gestão da Segurança da Informação) e a ISO/IEC 27001 (que aborda os

requisitos fundamentais para os sistemas de gestão da Segurança da Informação (ABNT, 2001; ABNT, 2005).

Por ser um tema bastante abrangente que envolve diversos contextos e está diretamente relacionado com o foco desta pesquisa, a Segurança da Informação merece destaque e será o assunto do tópico a seguir.

2.2 SEGURANÇA DA INFORMAÇÃO

Com um histórico recente que se combina com a Tecnologia da Informação, a Segurança da Informação é uma área de conhecimento que afeta tanto as organizações quanto as pessoas. A informação, que pode ser considerada um ativo para as organizações e algo de muito valor para as pessoas, carece de proteção contra os mais diversos tipos de vulnerabilidades (BEAL, 2005). Principalmente no mundo empresarial, informações compartilhadas e/ou armazenadas em meios eletrônicos estão expostas a inúmeros fatores que, mesmo sem intenção, oferecem risco às suas atividades. Podem ser exploradas as vulnerabilidades dos Sistemas de Informação de uma organização de forma com que suas informações organizacionais fiquem expostas a várias ameaças. Entre os alvos dessas ameaças estão o *hardware*, o *software*, os dados ou a rede de comunicação das empresas. A diversidade de alvos que podem ser atacados contribui para a importância da Segurança da Informação (WILSON, TURBAN e ZVIRAN, 1992).

Como um conceito inicial de Segurança da Informação, pode-se afirmar que ela diz respeito à proteção dos ativos da informação contra ameaças, tais como exposição não-autorizada, seja ocasional ou mal-intencionada, modificação, destruição, bem como sua indisponibilidade (WARD e SMITH, 2002), as quais exploram as vulnerabilidades dos sistemas de informação (WILSON, TURBAN e ZVIRAN, 1992). Expandindo o conceito inicialmente proposto, seguindo o ponto de vista organizacional, podemos dizer que Segurança da Informação é a proteção da informação contra as mais variadas ameaças, seja para garantir a manutenção da empresa, diminuir o risco empresarial, maximizar o retorno sobre os investimentos realizados ou aumentar as oportunidades de negócio (ABNT, 2005). Observa-se também que a Segurança da Informação possui três características que dizem respeito à preservação dos seguintes atributos fundamentais correlacionados (ABNT, 2001):

- Confidencialidade (ou Privacidade): garantia de que o acesso à informação seja feito somente por pessoal autorizado, assim como ter proteção conforme o grau de sigilo do seu conteúdo;

- Integridade: certeza de que a informação não foi alterada, seja de forma acidental ou intencional, assim como no seu processamento;
- Disponibilidade: garantia de que o pessoal autorizado tenha acesso à informação e aos recursos associados em momento oportuno.

De acordo com a visão de outros autores, mais elementos podem ser incluídos nesse aspecto. Sêmola (2003) acrescenta dois elementos aos anteriormente apresentados por considerar determinantes em uma informação:

- Legalidade: garantia de que a informação está de acordo com a legislação em vigor;
- Autenticidade (ou Confiabilidade): garantia da identidade dos elementos pertencentes a um determinado processo de comunicação eletrônica e de que a informação transmitida seja realmente a mesma que foi enviada.

Albertin e Pinochet (2010) ainda adicionam mais dois objetivos que podem ser considerados como parte do processo de Segurança da Informação:

- Consciência: certeza de que o sistema está funcionando conforme a expectativa dos usuários;
- Auditoria: proteger o sistema contra erros e ações cometidas por usuários autorizados.

Como a informação está presente em diversos processos de uma organização, as empresas devem considerar aspectos organizacionais e individuais que tratam e transformam a informação ao longo de todo o processo organizacional (LUCIANO, MAHMOOD e MAÇADA, 2010). No entanto, o reconhecimento de que a Segurança da Informação envolve uma interação complexa entre aspectos organizacionais, comportamentais e técnicos foi recentemente aceito (DUTTA e ROY, 2008).

Nos três itens a seguir, são apresentados os aspectos não-técnicos de Segurança da Informação considerados relevantes para o entendimento do tema de pesquisa em questão.

2.2.1 Aspectos Organizacionais Relativos à Segurança da Informação

Conforme a abordagem atual, que considera os aspectos organizacionais como parte do processo de gestão da Segurança da Informação, nota-se a importância da percepção dos colaboradores em relação ao ambiente organizacional para contribuir com o comportamento adequado dos funcionários referente à Segurança da Informação (WULFF, BERGMAN e

SVERKE, 2009), além da relevância dada pelos empregados às condições de trabalho apresentadas pelas organizações (DULEBOHN *et al*., 2009).

Seguindo os estudos de Wulff, Bergman e Sverke (2009), que identificaram a relação da satisfação do trabalho das pessoas com as habilidades, as técnicas e a concentração dos profissionais, Chan, Woon e Kankanhalli (2005) procuraram identificar o impacto do ambiente organizacional na Segurança da Informação, descobrindo relações relevantes entre o ambiente e a auto-eficácia dos funcionários em aderir às políticas práticas e controles de Segurança da Informação. A partir da percepção do clima organizacional, que é um conjunto de atributos específicos de uma determinada organização que pode ser induzida pela forma com que a empresa trata seus membros e seu ambiente, é possível verificar o relacionamento entre as características das condições de trabalho (políticas, práticas e controles de Segurança de Informação) e o comportamento individual no trabalho (CHAN, WOON e KANKANHALLI, 2005).

Nesse sentido, observa-se que, quando o ambiente de trabalho é considerado construtivo, os colaboradores entendem melhor seu papel no campo da Segurança da Informação organizacional, aumentando a conscientização em relação às ameaças de Segurança da Informação (SHAW *et al*., 2009). Consequentemente, quando o ambiente da organização for considerado desfavorável para o trabalho pelos funcionários, supõe-se que a aderência dos empregados por procedimentos e práticas de Segurança da Informação seja menor e origine vulnerabilidades a ameaças internas de Segurança da Informação.

As condições de trabalho oferecidas pelas organizações também é um fator a ser considerado na Segurança da Informação. Condições de trabalhos insatisfatórias podem contribuir negativamente para o trabalho (KELLOWAY *et al*., 2010), o que também pode ser identificado em casos onde a ansiedade e a incerteza estão presentes (BOZIONELOS, 2001). Cansaço e fadiga também são fatores que devem ser considerados, pois quando um indivíduo está cansado, sua atenção fica debilitada e políticas, práticas e controles de Segurança da Informação podem ser esquecidos ou desconsiderados (LUCIANO, MAHMOOD e MAÇADA, 2010).

Devido à grande concorrência no contexto empresarial, pressões por metas e por prazos em uma empresa são hábitos constantes. Porém, segundo Luciano, Mahmood e Maçada (2010), pressões no ambiente organizacional podem afetar as condições de trabalho, trazendo consequências indesejadas como a desconcentração, a desatenção, o stress e a ansiedade, que, consequentemente, também podem afetar a Segurança da Informação. Dentro dessa mesma situação, os estilos de liderança dos superiores também desempenham um papel

importante na conscientização dos funcionários relativo à Segurança da Informação e podem levar a um comportamento responsável relacionado à Segurança da Informação. (HUMAIDI e BALAKRISHNAN, 2015).

Já Albrechtsen (2007) observou que um alto volume de trabalho para garantir a proteção dos ativos informacionais gera um conflito de prioridades entre utilidade, eficiência e funcionalidade, o que também indica possíveis problemas relacionados com os aspectos organizacionais de Segurança da Informação. Para Albrechtsen e Hovden (2009), cargas excessivas de informações também podem comprometer o contexto de Segurança da Informação, pois o colaborador pode não estar preparado ou não ter um conhecimento inicial suficiente para absorver todo o conteúdo. Nesse mesmo sentido, Da Veiga e Eloff (2010) verificaram que Políticas de Segurança da Informação com linguagens técnicas, de difícil entendimento ou consideradas impraticáveis pelos empregados podem levar ao não cumprimento das regras e normas de Segurança, o que confirma a necessidade dos funcionários possuírem certas habilidades essenciais para garantir um ambiente relativamente seguro (WORKMAN, BOMMER e STRAUB, 2008). Uma tentativa a ser realizada pelas organizações é especificar bem (na Política de Segurança da Informação ou em outros meios de comunicação) quais objetos os colaboradores devem proteger através de seu comportamento (ANDERSON e AGARWAL, 2010).

A diminuição do nível de motivação de um funcionário também é um fator organizacional que deve ser considerado na Segurança da Informação. A baixa motivação dos colaboradores ocorre devido a diversas situações cotidianas pelo quais eles lidam, tais como falta de reconhecimento, ambiente de trabalho pouco desafiador, salário inadequado ou condições insatisfatórias para exercer a profissão, e afeta a identificação do funcionário com a organização, podendo acarretar também na falta de cuidado com políticas e procedimentos de Segurança da Informação, conforme os apontamentos de Luciano, Mahmood e Maçada (2010).

Assim, observa-se que sentimentos negativos dos funcionários podem estar relacionados com um ambiente organizacional sem condições de trabalho adequadas, o que, provavelmente, causará efeitos negativos para a gestão da Segurança da Informação nas organizações, assim como um mau exemplo de comportamento de colegas ou superiores pode servir de modelo para os outros envolvidos (LEACH, 2003) e afetar a Segurança da Informação.

Controles e monitoramento também são frequentemente implementados nas organizações para fins de Segurança da Informação com o objetivo de motivar colaboradores

a manterem um comportamento considerado adequado (BOSS *et al*., 2009). Como forma de garantir que os controles realmente funcionem na prática, boa parte das organizações recorrem ao uso da punição em caso de comportamento inadequado. Pode-se até impor a disciplina para manter a Segurança da Informação através do medo da punição ou da promessa de recompensa, mas os resultados dessas práticas tendem a não serem duradouros (LACEY, 2010).

Herath e Rao (2009a), em um estudo sobre o papel das penalidades, pressões e efetividade percebida no comportamento de Segurança da Informação nas organizações, verificaram que a certeza da detecção de uma violação, as crenças normativas (expectativa dos colegas ou pares que o indivíduo vai cumprir a Política de Segurança da Informação agrega mais chances da política realmente ser cumprida), o comportamento dos pares ou colegas e a efetividade percebida do seu próprio comportamento relativo à Segurança da Informação como um todo estão relacionados com a intenção de cumprir a Política de Segurança da Informação. No entanto, nessa mesma pesquisa, os autores não encontraram relação da severidade da punição no cumprimento da Política, pelo contrário, a severidade da punição favorece o não cumprimento das normas e regras da empresa. Em outra pesquisa de Herath e Rao (2009b), que abordou um modelo teórico mais complexo para motivação da proteção e dissuasão no comportamento de Segurança da Informação, também se obteve o mesmo resultado quanto à severidade da punição. Por isso, de acordo com Lacey (2010), a punição somente deve ser efetuada depois de esclarecidos os reais motivos dos erros e omissões dos funcionários, e isso só se as razões forem consideradas intencionais.

Com um modelo semelhante ao de Herath e Rao (2009a), porém mais antigo, D'Arcy, Hovav e Galletta (2008) introduziram o conceito de monitoramento de computadores como um dos precedentes da certeza e da severidade das sanções. Eles caracterizaram o monitoramento das atividades computacionais dos colaboradores como uma medida de segurança ativa que aumenta a capacidade da empresa em detectar erros e omissões, intencionais ou não, aumentando também a certeza e a frequência das punições, relação que foi comprovada cientificamente pelos autores. Assim sendo, isto pode indicar que o monitoramento dos empregados pode influenciar no comportamento relacionado à Segurança da Informação em uma organização. Entretanto, em estudo mais recente, D'Arcy e Hovav (2009), verificando os diferentes efeitos das contramedidas de Segurança da Informação nas intenções de uso indevido dos usuários, observaram que o julgamento sobre o comportamento ser certo ou errado tem mais influência do que Politicas de Segurança da Informação, programas de treinamento e monitoramento na intenção de um indivíduo promover um mau

uso de Sistemas de Informação, o que indica um dilema moral e ético no comportamento dos colaboradores.

Aspectos culturais, também incluídos no contexto organizacional, podem afetar a Segurança da Informação de maneira complexa e merecem atenção da área de estudo. Segundo os estudos de Kwantes e Boglarsky (2007), a cultura organizacional, constructo vindo da antropologia, causa efeito sobre o desempenho individual de cada colaborador e pode estar relacionada com o seu comportamento. Desta forma, fatores presentes na cultura organizacional devem manter uma estreita relação com o comportamento dos funcionários relativo a políticas, práticas e controles de Segurança da Informação, já que a cultura da organização pode ser condutora de práticas de Segurança da Informação (CHANG e LIN, 2007).

Vroom e Von Solms (2004) consideram cultura organizacional o padrão de pressupostos básicos que um determinado grupo inventou, descobriu ou desenvolveu em aprender a lidar com problemas de adaptação e integração na organização e que é repassado aos novos membros como a maneira adequada de se relacionar com esses problemas. Van Niekerk e Von Solms (2010) acrescentam que a cultura da organização considera três níveis: os artefatos (que podem ser facilmente notados), os valores expostos (valores que a organização preza e repassa para os seus membros) e as suposições tácitas ou crenças compartilhadas (convicção das pessoas de que as coisas devem funcionar de uma determinada maneira).

Com o objetivo de explorar potenciais problemas relacionados à tentativa de auditar o comportamento dos colaboradores, Vroom e Von Solms (2004) verificaram que os indivíduos reagem de maneira diferente de acordo com a situação vivenciada, dependendo da sua personalidade e de aspectos culturais intrínsecos da organização. Assim, observa-se que existe a necessidade de entender a interação entre a cultura organizacional e o comportamento, pois o comportamento individual é influenciado pela cultura organizacional e suas derivações do contexto organizacional (VROOM e VON SOLMS, 2004). Mais um indicativo disso pode ser a cultura de Segurança da Informação, definida como as atitudes, suposições, crenças, valores e conhecimento que os empregados utilizam para interagir com procedimentos, práticas e sistemas da organização, que pode resultar em comportamentos aceitáveis ou inaceitáveis na proteção dos ativos informacionais da organização (DA VEIGA e ELOFF, 2010). Portanto, uma gestão de Segurança da Informação eficiente somente pode ser alcançada através de uma observação mais próxima do comportamento humano (LACEY, 2010).

2.2.2 Comportamento Responsável Relativo à Segurança da Informação

Como visto anteriormente, colaboradores podem trazer grande danos à confidencialidade, integridade ou disponibilidade dos Sistemas de Informação através de atividades deliberadas ou gerar riscos pelo não cumprimento de políticas de Segurança da Informação, falta de atenção, treinamento insuficiente ou falta de motivação para proteger os ativos informacionais da organização (WARKENTIN e WILLISON, 2009). No entanto, Vroom e Von Solms (2004) afirmam que as violações da Política de Segurança da Informação são, em grande parte, devido à negligência ou à ignorância da Política por parte dos funcionários. A resistência dos colaboradores em cumprir práticas, procedimentos e regras de Segurança da Informação também é observada como um obstáculo para os gestores de Tecnologia da Informação, pois pode aumentar as chances de exposição a ameaças internas de Segurança da Informação (PUHAKAINEN e SIPONEN, 2010).

Diante disso, certos aspectos individuais podem estar relacionados com o comportamento responsável relativo à Segurança da Informação, compreendidos pela familiaridade dos funcionários com práticas, procedimentos e políticas de Segurança da Informação (RANSBOTHAM e MITRA, 2009), pela conscientização dos colaboradores em relação aos potenciais danos causados à organização em caso de alguma vulnerabilidade a ameaças internas de Segurança da Informação seja explorada (KRUGER e KEARNEY, 2006) e pelo comportamento avaliado como apropriado para uma gestão de Segurança da Informação efetiva (D'ARCY, HOVAY e GALLETTA, 2009). Na verdade, o comportamento dos empregados pode ser influenciado por diversos fatores, o que inclui o seu ambiente imediato, o comportamento dos pares, as demandas da gestão da empresa, sua experiência anterior e a percepção das consequências de suas ações (LACEY, 2010).

A confiança é um constructo relativamente difícil de ser mensurado. No entanto, o conceito de confiança tem sido muito utilizado em relações econômicas e sociais onde a incerteza, a delegação de autoridade e o medo do oportunismo são presenças constantes (CHO, 2006). Vindo de estudos da sociologia, a confiança na área de Segurança da Informação demonstra o sentimento dos colaboradores em relação às crenças de que as políticas práticas e controles funcionam corretamente e na influência do comportamento dos usuários relativos à Segurança da Informação de uma organização (LUCIANO, MAHMOOD e MAÇADA, 2010). Logo, a confiança é um aspecto individual de grande importância que afeta diretamente o comportamento do usuário em relação à Segurança da Informação.

Conhecimento e conscientização dos colaboradores apresentam um impacto positivo na satisfação com as medidas de Segurança da Informação, conforme Goodhue e Straub (1991), o que está relacionado com a familiaridade com aspectos de segurança, tais como políticas e procedimentos. A conscientização está relacionada com a mudança de atitude das pessoas, criando um clima mais satisfatório entre empregados, aumentando a motivação e tornando-os mais receptivos ao treinamento e às técnicas de supervisão e gerência, segundo Albertin e Pinochet (2010). Procurando identificar a efetividade da conscientização dos usuários de Segurança da Informação, Shaw *et al*. (2009) descobriu que a percepção e o entendimento dos usuários sobre assuntos de Segurança da Informação são fatores expressivos para garantir um ambiente de Tecnologia da Informação seguro.

Assim, o resultado do comportamento de colaboradores em relação à Segurança da Informação pode impactar na aderência a políticas, práticas e controles de segurança de uma organização, conforme Luciano, Mahmood e Maçada (2010). Ng, Kankanhalli e Xu (2008) descobriram em sua pesquisa que, quando as pessoas estão informadas sobre os danos causados por possíveis ameaças e da real possibilidade de sua ocorrência, elas se tornam mais conscientes em relação ao seu comportamento relacionado à Segurança da Informação.

A partir desse ponto de vista, nota-se a importância da estruturação de programas de conscientização como maneira de fazer as normas de Segurança da Informação serem cumpridas (SIPONEN, 2000). Conforme Kruger e Kearney (2006), a conscientização cria e mantém um comportamento positivo do funcionário, fazendo com que ele perceba a relevância do assunto em questão, pois sem a colaboração dos usuários, as metas da Segurança da Informação nunca poderão ser atingidas. Caso os funcionários não tenham um senso de posse com os principais ativos da empresa, a conscientização do comportamento pode ser uma maneira efetiva (ANDERSON e AGARWAL, 2010).

O gênero dos indivíduos também é um aspecto individual que pode ser considerado na Segurança da Informação. Venkatesh *et al.* (2003) incluiu, dentre outros aspectos, o gênero e a experiência como variáveis moderadoras no modelo UTAUT (Teoria Unificada de Aceitação e Uso de Tecnologia), confirmando a variação do gênero e da experiência como um aspecto que pode influenciar na intenção comportamental dos usuários de Sistemas de Informação. A experiência que ele tem no desempenho de seu trabalho e a lealdade dele relativo à organização em que ele trabalha são aspectos individuais que também são ponderados em trabalhos recentes sobre Segurança da Informação (LACEY, 2009). Albrechtsen e Hovden (2009) acrescentam experiência em Tecnologia da Informação, nível de escolaridade e cargo desempenhado no trabalho como aspectos individuais que impactam

no comportamento do usuário relativo às políticas, práticas e controles de Segurança da Informação.

2.3 VULNERABILIDADES A AMEAÇAS INTERNAS DE SEGURANÇA DA INFORMAÇÃO

Todo e qualquer sistema de informação organizacional possui vulnerabilidades que podem ser exploradas por diversos tipos de ameaças (GUPTA *et al.*, 2006), tanto internas quanto externas. Conforme esses autores, as organizações utilizam a gestão da Segurança da Informação para reduzir os potenciais riscos de dano que essas vulnerabilidades podem causar na empresa e que podem impactar nos negócios da organização através da perda de confidencialidade, integridade e disponibilidade das informações. De acordo com quase todos os autores especializados nesta área citados na pesquisa, os incidentes de Segurança da Informação provocados por ameaças internas superam os que foram gerados por ameaças externas. Logo, proteger contra as chances de exposição a ameaças internas pode ser a melhor alternativa de manter um ambiente relativamente seguro.

Uma ameaça interna pode ser definida como o potencial de uma fonte interna específica com motivação, capacidade e oportunidade de obter sucesso ao explorar uma determinada vulnerabilidade ou comprometer um sistema (SARKAR, 2010). Como as ameaças internas abrangem uma série de eventos, incidentes e ataques que trazem riscos imensos causados por usuários autorizados de Tecnologia da Informação (LEACH, 2003) e são consideradas as que mais têm oportunidades e vantagens para acessar ativos importantes da organização, além de ter o conhecimento de como coletar uma informação valiosa e como encobrir suas ações (JAAFAR e AJIS, 2013), isso tudo eleva ainda mais a importância da proteção contra vulnerabilidades a ameaças internas de Segurança da Informação. Assim como os Sistemas de Informação, que não são plenamente protegidos, a ameaça interna é um problema único e nunca poderá ser totalmente eliminada (SARKAR, 2010), os esforços são apenas para minimizar ao máximo as vulnerabilidades.

Pode-se entender vulnerabilidade como as fraquezas associadas a ativos que processam informações que, sendo exploradas por ameaças, permitem o surgimento de um incidente de Segurança da Informação (SÊMOLA, 2003). Seguindo essa mesma lógica, Sarkar (2010) define vulnerabilidade como uma medida da capacidade de exploração de uma fraqueza que engloba os processos de negócio, os sistemas de comunicação e a Tecnologia da Informação da organização. Alguns autores, como Albrechtsen e Hovden (2009), citam os

funcionários como uma vulnerabilidade em potencial, já que muitos podem não ter conhecimentos e habilidades suficientes para garantirem um comportamento adequado à Segurança da Informação.

É importante ressaltar que uma vulnerabilidade em si não causa necessariamente um incidente ou evento de Segurança (SOLTANMOHAMMADI, ASADI e ITHNIN, 2013), assim como uma violação da Política de Segurança da Informação pode não acarretar em uma vulnerabilidade propriamente dita (KRAEMER e CARAYON, 2007), mas ela deve ser prevenida ou protegida para não ser explorada por ameaças internas. No entanto, existem correntes contrárias, tais como Bulgurcu, Cavusoglu e Benbasat (2010), que consideram toda e qualquer violação da Política de Segurança da Informação provocada pelos colaboradores como vulnerabilidade, mesmo sem incorrer nenhuma chance de incidente. Assim, vulnerabilidade pode ser caracterizada como a suscetibilidade de exposição a uma ameaça que pode causar um evento de Segurança da Informação, caso medidas de proteção não forem adotadas (VANCE, SIPONEN e PAHNILA, 2012).

Nesse mesmo contexto, surge o conceito de brecha de Segurança da Informação. Kraemer e Carayon (2007), em estudo sobre erros humanos e violações de segurança, conceituam brechas de Segurança da Informação como um resultado não autorizado da exploração de uma vulnerabilidade latente, consequência de um evento resultante de uma ação não sancionada (ou seja, erro humano, intencional ou não) por um usuário do sistema. Por exemplo, utilizar um mesmo usuário e senha para diversas contas de acesso a Sistemas de Informação diferentes de uma organização pode gerar uma vulnerabilidade a ameaças internas de Segurança da Informação (BANG *et al.* 2012), porém, somente é considerada uma brecha de Segurança da Informação quando esse usuário e senha foi utilizado por outra pessoa, a não ser o próprio usuário. Logo, a brecha de Segurança da Informação é um incidente que já aconteceu a partir da exploração de uma determinada vulnerabilidade por uma ameaça.

Quanto às categorias de vulnerabilidades dos Sistemas de Tecnologia da Informação, Gupta *et al.* (2006) consideram as seguintes:

- Inerente ao Desenho/Arquitetura: Singularidade, centralização, separabilidade e homogeneidade;
- Complexidade Comportamental: Sensibilidade e previsibilidade;
- Adaptação e Manipulação: Rigidez, maleabilidade e ingenuidade;
- Operação/Configuração: Limites da Capacidade, falta de recuperação, falta de auto-conscientização, dificuldade de gerenciamento e complacência;

- Exposição Indireta/Não-física: Acessibilidade e transparência;
- Exposição Direta/Física: Acessibilidade física e susceptibilidade eletromagnética; e
- Suporte às Instalações/Infraestruturas: Dependência.

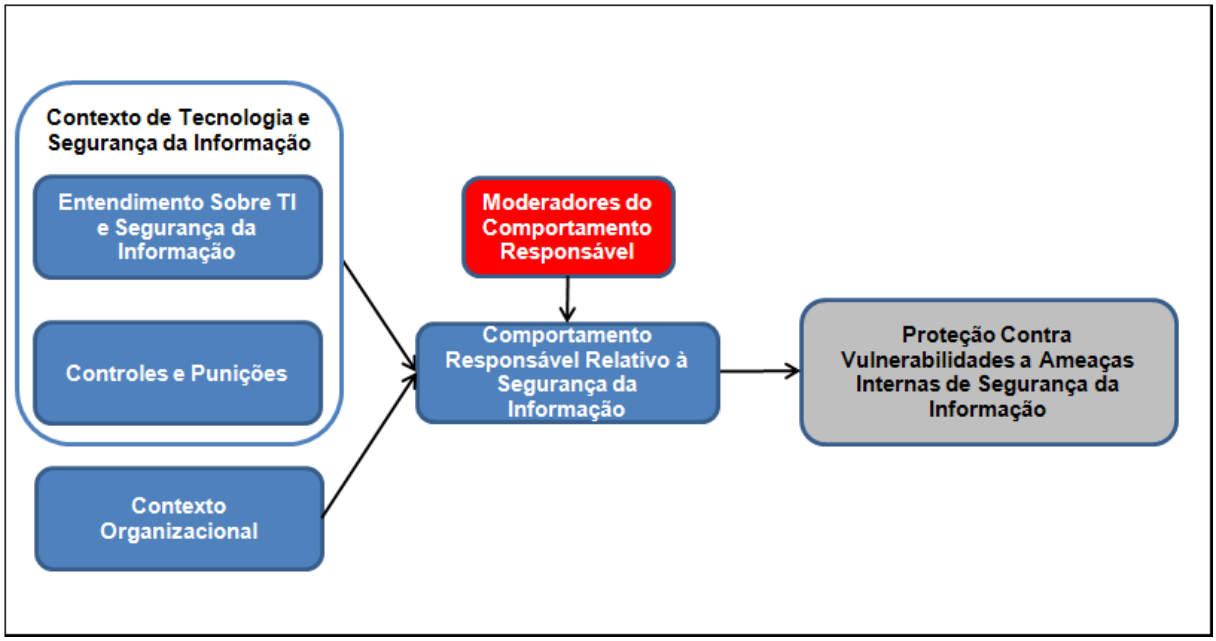
Kraemer e Carayon (2007) classificam os tipos de erros humanos e identificou elementos organizacionais e individuais que contribuem para a Segurança da Informação. Como resultado desse estudo, os autores verificaram indícios de que fatores como comunicação, cultura de segurança e estrutura organizacional tendem a influenciar nos erros, acidentais ou intencionais, dos funcionários, o que leva ao aumento dos riscos em relação às vulnerabilidades a ameaças internas de Segurança da Informação observadas. A priorização de outras tarefas ao invés dos procedimentos de Segurança da Informação também é um erro humano que pode propiciar vulnerabilidades a ameaças internas (ALBRECHTSEN, 2007), assim como facilitar a incidência de brechas de privacidade (LIGINLAL, SIM e KHANSA, 2009).

Diante de todas essas vulnerabilidades dos Sistemas de Tecnologia da Informação que podem atingir as organizações, a necessidade de um estudo aprofundado sobre os aspectos envolvidos nas vulnerabilidades a ameaças internas de Segurança da Informação se mostra ainda mais relevante.

2.4 MODELO CONCEITUAL

Baseado na fundamentação teórica desta pesquisa, foi criado um modelo conceitual que servirá de apoio para o desenvolvimento deste estudo (ver Figura 1). O modelo é focado em aspectos comportamentais de Segurança da Informação, basicamente nos contextos organizacional e de Tecnologia e Segurança da Informação e suas possíveis relações de influência no comportamento responsável dos colaboradores relacionado à Segurança da Informação com a finalidade de evitar vulnerabilidades a ameaças internas de Segurança da Informação. Cada construto do modelo conceitual representa uma das dimensões estudadas na pesquisa e cada seta sugere uma possível relação de influência entre os construtos no sentido indicado.

Figura 1: Modelo conceitual proposto



Fonte: O autor (2014)

Como contexto de Tecnologia e Segurança da Informação, entende-se que sejam os fatores de Tecnologia da Informação e de Segurança da Informação da empresa que podem afetar, direta ou indiretamente, os funcionários. Para facilitar o entendimento e a abordagem desse contexto, ele foi dividido em duas partes: Entendimento sobre TI e Segurança da Informação e Controles e Punições. Entendimento sobre TI e Segurança da Informação diz respeito à compreensão proporcionada pela organização ou já garantida pelos empregados frente a assuntos gerais de Tecnologia da Informação e Segurança da Informação, tais como conhecimentos, habilidades e experiência em Tecnologia da Informação e conhecimento e severidade da Política de Segurança da Informação. Já Controles e Punições aborda os controles utilizados e as punições previstas pela empresa aos colaboradores em situações que possam prejudicar a Segurança da Informação, o que está relacionado aos mecanismos de controle utilizados para garantir a Segurança da Informação, o monitoramento das atividades realizadas e as punições previstas ou efetivadas.

Quanto ao contexto organizacional, podemos caracterizar como o ambiente da organização a que os colaboradores pertencem, o que inclui o clima e a cultura organizacional, o fluxo de trabalho, as relações entre colaboradores e superiores, as condições de trabalho oferecidas, os tipos de ambiente organizacional, o comportamento dos pares e a satisfação individual com o trabalho.

No que diz respeito ao Comportamento Responsável relativo à Segurança da Informação, refere-se ao comportamento definido como adequado pela organização e que se recomenda ou se espera ser concretizado pelos colaboradores, o que abrange formas de disseminação do comportamento, treinamentos e programas de conscientização e capacitação, uso da Política de Segurança como mecanismo de proteção, juízo de comportamento frente à Política de Segurança e a seriedade, a prejudicialidade e a legitimidade da violação de regras e normas de Segurança. Como Moderadores do Comportamento Responsável, entende-se àqueles fatores que podem controlar o comportamento responsável dos funcionários em relação à Segurança da Informação, referidos no modelo como o gênero, a lealdade à empresa, a escolaridade e o nível hierárquico.

Por fim, considera-se Proteção contra Vulnerabilidades a Ameaças Internas de Segurança da Informação todos os esforços, práticas ou procedimentos que a organização realiza para evitar chances de exposição a ameaças vindas de dentro da própria empresa. Assim sendo, de acordo com o modelo conceitual proposto, considera-se que os Contextos Organizacional e de Tecnologia e Segurança da Informação (Entendimento sobre TI e Segurança da Informação e Controles e Punições) influenciam no Comportamento Responsável dos funcionários relativo à Segurança da Informação que, por consequência, influencia na Proteção contra Vulnerabilidades a Ameaças Internas de Segurança da Informação. Como complemento do modelo conceitual, os Moderadores do Comportamento Responsável apresentam um conjunto de variáveis que podem afetar diretamente o controle do Comportamento Responsável dos colaboradores relativo à Segurança da Informação.

Assim, nota-se que o modelo conceitual desenvolvido a partir da literatura referenciada busca identificar e entender a relação de influência dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável dos funcionários visando evitar vulnerabilidades a ameaças internas de Segurança da Informação.

3 MÉTODO DE PESQUISA

Este capítulo visa esclarecer o método de pesquisa utilizado nesta pesquisa. A seguir, serão apresentados o delineamento metodológico da pesquisa, a coleta de dados utilizada, bem como a análise de dados. O delineamento do estudo diz respeito aos procedimentos metodológicos utilizados na pesquisa, o que contempla a abordagem, a estratégia, o método, a unidade de análise e o desenho de pesquisa. A coleta de dados apresenta as técnicas utilizadas para coletar os dados, ou seja, entrevistas semi-estruturadas, bem como a elaboração, a validação e a aplicação do roteiro de entrevistas, além do perfil e do número de entrevistados. A técnica de análise de conteúdo será o tema presente no tópico de análise de dados.

3.1 DELINEAMENTO METODOLÓGICO

De acordo com a visão de Hair Jr. *et al*. (2005), método científico é aquele que os pesquisadores utilizam para buscar conhecimento em um tema definido. Isso envolve pensamento lógico e cognição, fundamentos com capacidade de solidificar o processo de conhecimento científico, resolvendo os problemas encontrados e atingindo os objetivos do projeto de pesquisa em questão. Desta forma, o método envolve um conjunto de atividades e técnicas desenvolvidas para investigar um determinado fenômeno.

A pesquisa científica parte do pressuposto que existem dois tipos de enfoques ou abordagens gerais, que classifica os dados da pesquisa de maneira quantitativa e qualitativa (SAMPIERI, COLLADO e LUCIO, 2006). Segundo esses autores, a abordagem quantitativa utiliza técnicas de coleta e análise de dados para testar hipóteses instituídas de acordo com a questão de pesquisa do estudo, com o emprego de medições numéricas e apoio de análises estatísticas para instituir padrões de comportamento de uma população. Já o enfoque qualitativo usa coleta de dados não-quantitativas, tais como entrevistas, observações e revisões documentais, e, geralmente, apresenta hipóteses ou proposições de pesquisa a serem testadas como resultado do estudo (SAMPIERI, COLLADO e LUCIO, 2006).

Para a realização desta pesquisa, o enfoque qualitativo foi considerado o mais adequado e foi a abordagem de pesquisa utilizada. A pesquisa qualitativa tem como objetivo conseguir uma compreensão qualitativa sobre as razões pelo qual acontece o problema pesquisado, os dados qualitativos são coletados com o intuito de que se consiga conhecer melhor os fatores que não podem ser observados e medidos diretamente, além de que a abordagem qualitativa considera aspectos interpretativos e subjetivos das realidades sociais.

Segundo Sampieri, Collado e Lucio (2006, p. 11), “um estudo qualitativo busca compreender seu fenômeno de estudo em seu ambiente usual”. Para explicar a pesquisa qualitativa, Roesch (2009) afirma que sua base vem do paradigma fenomenológico, já que o mundo é diversificado, composto por indivíduos distintos que respondem de formas diferentes a uma situação idêntica. Ambos autores citados acima justificam a escolha dessa abordagem para esta pesquisa.

Quanto às estratégias de pesquisa, Sampieri, Collado e Lucio (2006) ressaltam a existência de quatro tipos de estratégias: a explicativa, a correlacional, a descritiva e a exploratória. De maneira geral, a estratégia de pesquisa explicativa identifica fatores que causam determinadas situações com o objetivo de entender um fenômeno, a pesquisa do tipo correlacional explica parcialmente um problema relacionando dois ou mais conceitos a cerca de um tema, o estudo descritivo consiste em descrever características de grandes amostras para expor como um fenômeno se manifesta por completo e a estratégia de pesquisa exploratória consiste em examinar um tema de pesquisa pouco estudado para buscar uma imersão inicial no assunto, aprimorando ideias e confirmando teorias ou percepções (SAMPIERI, COLLADO e LUCIO, 2006). Conforme as estratégias de pesquisa apresentadas, o tipo exploratório se constitui como o mais indicado para esse estudo e, portanto, foi a estratégia adotada. Para Aaker, Kumar e Day (2004), a pesquisa exploratória é utilizada para se buscar um maior entendimento sobre a natureza do problema estudado, as possíveis hipóteses alternativas e as variáveis relevantes que devem ser consideradas, o que apóia a escolha da estratégia de pesquisa exploratória para este estudo.

A partir da escolha da estratégia de pesquisa, é necessário definir o método de pesquisa a ser utilizado em um estudo qualitativo. Yin (2007) ressalta três tipos de métodos de pesquisa mais adequados para coletar dados qualitativos: a pesquisa-ação, o estudo etnográfico e o estudo de caso. Entretanto, Marconi e Lakatos (2011) também consideram as entrevistas como um método de pesquisa muito utilizado em estudos qualitativos, o que é justificável quando se investiga o ponto de vista ou as experiências dos indivíduos, compreendendo plenamente a pesquisa em questão. Para Vergara (2012), a entrevista é um método de pesquisa que, quando executada adequadamente, agrega à pesquisa informações coerentes e consistentes que podem fornecer resultados relevantes para o campo. Sendo assim, decidiu-se adotar a entrevista, pois ela é o método de pesquisa mais apropriado e caracterizado para esta pesquisa.

Portanto, esta dissertação foi realizada por meio de entrevistas em uma única etapa exploratória que, com a aplicação de um roteiro de entrevistas semi-estruturadas, buscam

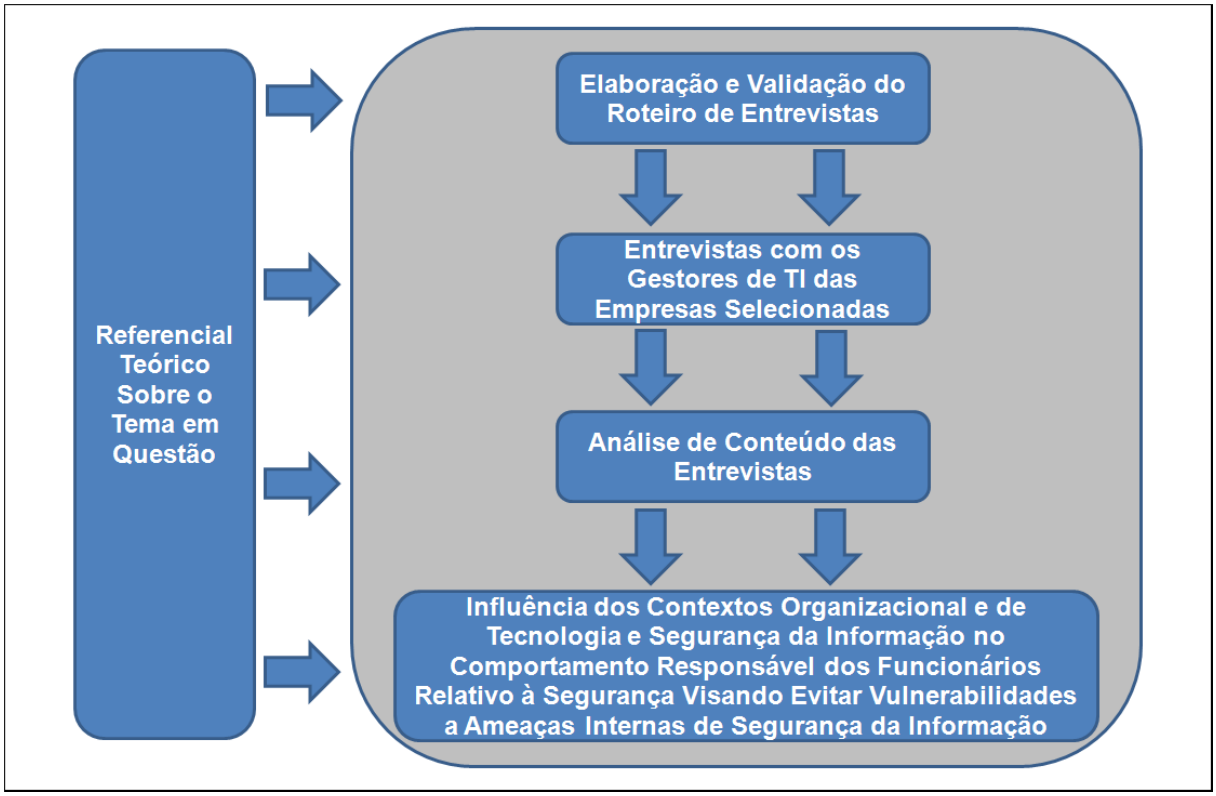
identificar e analisar a influência dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável relativo à Segurança da Informação visando proteger contra vulnerabilidades a ameaças internas de Segurança da Informação, de acordo com a percepção dos gestores de TI das organizações envolvidas. Inicialmente, foi prevista também a utilização de pesquisa documental, a partir da análise das políticas de Segurança da Informação das organizações a que os gestores pertenciam, para fins de triangulação e cotejamento dos dados, bem como forma de complementação do estudo. Entretanto, a análise documental foi descartada, pois apenas um pequeno número de organizações disponibilizou suas respectivas políticas de Segurança da Informação alegando, mesmo com a garantia de anonimato em toda a pesquisa, ser um documento interno e, portanto, confidencial. Logo, um possível estudo de caso foi descaracterizado e, por esse motivo, optou-se pelo método de pesquisa por entrevistas no estudo em questão.

Diante das alternativas de tempo de análise indicadas por Sampieri, Collado e Lucio (2006), a de corte transversal e a de corte longitudinal, optou-se pelo corte do tipo transversal, ou seja, uma única análise em um determinado momento do tempo.

O objeto de uma pesquisa é a unidade de análise e está relacionada diretamente com a questão definida no problema de pesquisa (YIN, 2007). Assim, apesar da pesquisa utilizar a percepção dos gestores de TI das empresas analisadas como forma de obter os dados necessários para a análise do estudo, a unidade de análise que deve ser considerada são as práticas ou os esforços utilizados para garantir o comportamento adequado dos funcionários relacionado à Segurança da Informação.

Abaixo, encontra-se o desenho de pesquisa utilizado nesta dissertação, visando situar as etapas e os procedimentos metodológicos adotados (ver Figura 2).

Figura 2: Desenho de pesquisa



Fonte: O autor (2014)

As técnicas de coleta e análise de dados desta dissertação serão apresentadas nos dois tópicos que se seguem.

3.2 COLETA DE DADOS

A técnica que foi utilizada na coleta de dados dessa pesquisa exploratória é a entrevista semi-estruturada, a ser detalhada a seguir. A elaboração, validação e aplicação do roteiro de entrevistas também constam neste item, assim como as dimensões e as variáveis estudadas e os requisitos para a escolha das empresas a serem pesquisadas.

Segundo a explicação de Flick (2004), a entrevista semi-estruturada apresenta um grau de estruturação básico, com questões-chave pré-elaboradas pelo entrevistador. Ainda segundo o autor, o entrevistado tem a liberdade de falar o quanto quiser sobre o tema em questão e o entrevistador pode complementar com questões que não estavam no roteiro ou até mesmo omitir alguma, conforme o andamento da entrevista ou caso acredite ser necessário.

Neste tipo de entrevista, o entrevistado deve ter conhecimento específico sobre o tema em questão, incluindo "... suposições que são explícitas e imediatas, as quais ele pode expressar espontaneamente ao responder uma pergunta aberta, e que são complementadas por

suposições implícitas" (FLICK, 2004, p. 95). Aaker, Kumar e Day (2004) afirmam que as entrevistas semi-estruturadas são focadas em determinados temas, fazendo com que o respondente tenha uma liberdade relativamente menor, pois ela busca seguir uma série de assuntos pré-direcionados.

As entrevistas semi-estruturadas seguiram o roteiro de entrevistas definido na pesquisa (ver Apêndice A). Todas as entrevistas foram gravadas em áudio, com a devida permissão concedida de todos os entrevistados, para garantir a fidelidade do estudo e auxiliar na análise de dados, chegando a quase 14 horas de gravação. É importante salientar que o anonimato do entrevistado, bem como da empresa onde ele trabalha, foi mantido em todo o projeto.

A partir da literatura referenciada do assunto em questão, tendo como fundamento o modelo conceitual proposto, elaborou-se a primeira versão de um roteiro de entrevistas semi-estruturadas para coletar dados de gestores de Tecnologia da Informação que trabalham nas organizações selecionadas na pesquisa. No entanto, houve a necessidade da criação de algumas outras questões relacionadas ao tema de pesquisa, pois não foram encontradas referências na revisão teórica e a inclusão delas era de extrema importância para o estudo. As oito novas questões incluídas são as que apresentam o autor como principal fonte de referência das variáveis indicadas no quadro disponibilizado a seguir (Quadro 1 - Quadro de Dimensões e Variáveis) e outras informações complementares podem ser verificadas no Apêndice B.

Com a criação de um quadro de dimensões e variáveis, foi dado o início da elaboração do roteiro de entrevistas semi-estruturado. As dimensões utilizadas foram: Contexto Organizacional, Contexto de Tecnologia e Segurança da Informação (sendo essa subdividida em outras duas dimensões, Entendimento sobre TI e Segurança da Informação e Controles e Punições, para melhor entendimento e facilidade de análise), Comportamento Responsável relativo à Segurança da Informação e Moderadores do Comportamento Responsável (ver Quadro 1). Quanto às variáveis da pesquisa, 28 foram abordadas, mesmo número de questões do roteiro de entrevistas final, sendo uma questão para cada variável da pesquisa (ver Apêndice B).

Quadro 1: Quadro de Dimensões e Variáveis

DIMENSÕES		VARIÁVEIS	PRINCIPAIS FONTES
Contexto de Tecnologia e Segurança da Informação	**Entendimento sobre TI e Segurança da Informação**	Conhecimento e Habilidades	Workman, Bommer e Straub (2008)
		Experiência e Conhecimentos Gerais em TI	Lacey (2009)
		Conhecimento da Política de Segurança da Informação	Lee, Lee e Yoo (2004)
		Severidade da Política de Segurança da Informação	Herath e Rao (2009a)
	Controles e Punições	Mecanismos de Controle como Inibidores do Desempenho e da Criatividade	O autor (2014)
		Mecanismos de Controle da Violação de Regras e Normas	O autor (2014)
		Punição como Inibidor da Reincidência de Eventos de Segurança da Informação	Herath e Rao (2009a)
		Monitoramento	D'Arcy, Hovav e Galletta (2008) e Herath e Rao (2009a)
		Monitoramento como Inibidor de Eventos de Segurança da Informação	D'Arcy, Hovav e Galletta (2008) e Herath e Rao (2009a)
Contexto Organizacional		Clima Organizacional	Chan, Woon e Kankanhalli (2005)
		Fluxo de Trabalho de Segurança da Informação	Albrechtsen (2007)
		Cultura Organizacional	Chang e Lin (2007)
		Relação entre Funcionários e seus Superiores	Vroom e Von Solms (2004) e Shaw *et al*. (2009)
		Condições de Trabalho	Bozionelos (2001) e Kelloway *et al*. (2010)
		Diferenças entre Ambientes Organizacionais	Mikkelsen (2002) e Dulebohn (2009)
		Comportamento dos Pares	Herath e Rao (2009a)
		Satisfação com o Trabalho	Stanton *et al*. (2004)
Comportamento Responsável Relativo à Segurança da Informação		Disseminação do Comportamento	O autor (2014)
		Treinamento, Capacitação e Conscientização	Lee, Lee e Yoo (2004)
		Política de Segurança da Informação como Mecanismo de Proteção	O autor (2014)
		Juízo de Comportamento Relacionado à Política de Segurança da Informação	O autor (2014)
		Seriedade da Violação de Regras e Normas	Lee, Lee e Yoo (2004)
		Prejudicialidade da Violação de Regras e Normas	Lee, Lee e Yoo (2004)
		Legitimidade da Violação de Regras e Normas	Lee, Lee e Yoo (2004)
Moderadores do Comportamento Responsável		Gênero	O autor (2014)
		Lealdade à Empresa	Lacey (2009)
		Escolaridade	O autor (2014)
		Nível Hierárquico	O autor (2014)

Fonte: O autor (2014)

Depois de realizada a elaboração do roteiro de entrevistas, foi feita a validação de face e de conteúdo. A validação do roteiro de entrevistas serve para verificar se o conteúdo

abordado e a estrutura proposta estão de acordo com o objetivo do instrumento (COOPER e SCHINDLER, 2003). Para a validação deste roteiro de entrevistas, foram consultados cinco profissionais do meio acadêmico, todos com doutorado, vasta experiência na área de Tecnologia da Informação e conhecimento específico em Segurança da Informação e Metodologia de Pesquisa. A validação do roteiro foi feita individualmente com cada um dos avaliadores, abordando os objetivos e a estrutura do roteiro, bem como o entendimento para o público-alvo e a conduta durante as entrevistas a serem realizadas. Algumas observações foram feitas pelos especialistas, principalmente mudanças na abordagem das questões, que foram positivas para a definição do roteiro de entrevistas final e devidamente adotadas.

A última etapa de validação do instrumento foi a realização do pré-teste, que contou com a participação de dois especialistas na área de Segurança da Informação diferentes dos avaliadores iniciais do instrumento, mas com o mesmo perfil dos prováveis respondentes da pesquisa, no qual duas entrevistas foram simuladas nos sentido de verificar a compreensão dos respondentes em relação ao instrumento e de garantir o atendimento ao objetivos da pesquisa, além de testar a abordagem do entrevistador (no caso, o próprio autor da pesquisa) frente ao assunto. Pequenas considerações foram feitas relativas ao pré-teste, apenas mudanças superficiais na forma de abordagem das perguntas para facilitar o entendimento dos entrevistados, tais como mudança na linguagem das questões para uma mais adequada à realidade dos pesquisados e melhora do apoio teórico do entrevistador para ilustrar melhor as questões abordadas. Assim, o roteiro de entrevistas final foi dado como concluído, contando com 28 questões relacionadas às dimensões e variáveis apresentadas no quadro anterior (ver Quadro 1) e seis questões para caracterização dos respondentes. O roteiro de entrevistas completo utilizado encontra-se no Apêndice A, disponível no final do trabalho.

A partir da validação do instrumento, foi realizada a sua aplicação nas entrevistas. Pretendia-se realizar as entrevistas com a aplicação do roteiro de entrevistas semi-estruturadas com quinze gestores de Tecnologia da Informação (CIOs - *Chief Information Officers* ou responsáveis pela Segurança da Informação) de quinze grandes organizações diferentes que utilizam de forma intensiva a Tecnologia da Informação e que precisam manter esforços permanentes em relação à Segurança da Informação. O que definiu os gestores de Tecnologia da Informação como os mais adequados para responderem a essas questões foi o fato de que eles são os mais qualificados quanto ao assunto abordado, pois possuem uma visão holística da organização e conhecimento técnico específico sobre Segurança da Informação, algo que o colaborador ou o usuário comum em geral, não tem. Utilizando como base a classificação das 100 maiores empresas do Rio Grande do Sul no ano de 2010, foi verificada a disponibilidade

de cada organização em participar da pesquisa a partir da primeira colocada no ranking, e assim, foi utilizado o critério de conveniência das empresas disponíveis à realização da entrevista pelo pesquisador. Como dito anteriormente, todas as entrevistas foram gravadas em áudio para posterior transcrição e facilitação na análise de dados, sendo que o anonimato dos entrevistados foi garantido, bem como a permissão para gravação das entrevistas. No fim, catorze foi o número final de entrevistas consolidadas.

3.3 ANÁLISE DE DADOS

Depois de encerrada a fase de coleta de dados da pesquisa qualitativa, de acordo com Roesch (2009), o pesquisador obtém uma quantidade imensa de dados na forma de texto, que terão de ser organizados e interpretados. Quanto à organização desses dados, a maneira mais utilizada é a codificação de forma categorial ou temática, que nada mais é do que a contagem de uma ou diversas categorias de significação em uma unidade de codificação previamente determinada (BARDIN, 2011). Assim, segundo a autora, é possível fornecer uma representação simplificada dos dados brutos, com capacidade de sintetização de partes significativas de um texto que foram desmembradas e reagrupadas em forma de unidades categoriais, facilitando a compreensão e a interpretação dos dados. A codificação por categorias separa diferentes trechos considerados relevantes de um ou de vários documentos que, apesar de serem distintos, estão relacionados entre si por constarem da mesma ideia ou tema central, atribuindo-lhes um código exclusivo.

Para interpretar estes dados codificados, Roesch (2009) cita que existem três tipos de análise: análise de conteúdo, construção de teoria e análise de discurso. Para Bardin (2011), análise de conteúdo é um conjunto de técnicas de análise das comunicações que pode ser utilizada tanto para entrevistas quanto para pesquisas documentais. Os textos gerados na transcrição das entrevistas realizadas nesta pesquisa foram avaliados através do método de análise de conteúdo do tipo categorial ou temática, pois toda a codificação categorial ou temática feita a partir de uma transcrição simplifica e facilita o processo de análise (GIBBS, 2009). Segundo Roesch (2009), os procedimentos desse método de análise buscam levantar informações relevantes por meio da classificação de palavras, frases e parágrafos em categorias de conteúdo relevante. Dentre as diversas técnicas de análise de conteúdo, a análise do tipo categorial, que constitui do destaque de partes de um texto em unidades de registros para categorizar em grupos analógicos, foi a que melhor delimitou a pesquisa. Para Bardin (2011), esta é a primeira etapa da análise de conteúdo e consiste na codificação das unidades

de registros para descobrir os núcleos de sentido cuja frequência de aparição possa significar algo relevante para o estudo. Para avaliar as unidades de registro, a autora propõe a utilização de regras de enumeração, sendo que a mais significativa é a frequência com que uma unidade de registro aparece no texto e foi utilizada nesta pesquisa.

Para fins de detalhamento da análise de dados adotada nesta pesquisa, a partir da transcrição completa e fidedigna de todas as entrevistas realizadas (cerca de 200 páginas), foi feita uma categorização temática por meio das questões aplicadas, ou seja, pela variável que foi atribuída a cada questão. Em seguida, foi feita uma análise categorial baseada nas afirmações ou nas negações da relação de influência percebida pelos gestores em cada uma das variáveis/questões. Posteriormente, nas três etapas de análise subsequentes, cada trecho relevante das respostas dos entrevistados em cada questão ou variável atribuída foi separado e reagrupado em outras categorias temáticas que representavam um mesmo assunto ou conceito dentro da mesma variável/questão, utilizando o *software* Sphinx Survey Edição Léxica V5 para análise de conteúdo como forma de auxiliar na categorização dos dados e agilizar a análise dos dados em si, o que, praticamente, diminuiu o conteúdo inicialmente transcrito pela metade (algo em torno de 110 páginas). A partir dessa codificação, foi possível identificar a relação de influência percebida dos contextos organizacional e de Tecnologia e Segurança da Informação no comportamento responsável dos empregados relacionado à Segurança da Informação visando proteger contra vulnerabilidades a ameaças internas de Segurança da Informação por meio da frequência de observações e do total de evidências encontradas em cada categoria. Na última etapa da análise, foi possível evidenciar os fatores desencadeadores do comportamento individual e organizacional acerca das vulnerabilidades a ameaças internas de Segurança da Informação, a partir da união das duas categorias mais citadas pelos gestores em cada variável da etapa de análise da relação de influência dos Contextos no Comportamento Responsável dos funcionários relativo à Segurança da Informação. No próximo capítulo, todos os resultados da análise de conteúdo explicada aqui são definitivamente apresentados.

4 RESULTADOS

Neste capítulo são apresentados os resultados obtidos a partir da análise dos dados coletados no estudo por meio da aplicação do roteiro de entrevistas anteriormente detalhado e que se encontra disponível no Apêndice B. Este item está dividido nas seguintes seções: Caracterização das Empresas e dos Respondentes; Contexto de Tecnologia e Segurança da Informação e Comportamento Responsável Relativo à Segurança da Informação; Contexto Organizacional e Comportamento Responsável Relativo à Segurança da Informação; Comportamento Responsável Relativo à Segurança da Informação e Vulnerabilidade a Ameaças Internas de Segurança da Informação; e Fatores Desencadeadores do Comportamento Responsável Relativo à Segurança da Informação.

4.1 CARACTERIZAÇÃO DAS EMPRESAS E DOS RESPONDENTES

Esta etapa constitui-se da caracterização das organizações estudadas na pesquisa, bem como dos entrevistados que respondiam pelas empresas. De acordo com o perfil inicialmente estabelecido e demonstrado no capítulo anterior sobre a metodologia de pesquisa utilizada no trabalho, foram selecionadas as empresas a serem analisadas. Como comentado anteriormente, foi mantida a confidencialidade das empresas e dos seus respectivos respondentes. A caracterização foi feita apenas para confirmar que o perfil inicial da pesquisa foi cumprido, assim como a experiência do profissional na área de interesse do trabalho. Logo, nenhum nome ou caracterização profunda foi realizada, somente aspectos gerais foram especificados. A caracterização das organizações diz respeito ao ramo de atuação, ao porte da empresa e às questões 1 a 4 da etapa sócio-demográfica do roteiro de entrevistas, que tratam sobre o número de funcionários, o número de funcionários que utilizam computadores, o percentual do faturamento investido em Tecnologia da Informação e os regulatórios em que a empresa está sujeita, respectivamente. O Quadro 2 localizado abaixo apresenta a caracterização simplificada das organizações que participaram da pesquisa.

Quadro 2: Caracterização das empresas pesquisadas

Organizações Estudadas	Ramo de Atuação	Porte da Empresa	Nº de Colaboradores	Nº de Colaboradores Usando Computadores	Percentual do Faturamento Investido em TI	Regulatórios
Empresa A	Serviços	Grande	500	400	8%	Não
Empresa B	Indústria	Grande	300	200	2%	Auditorias internas
Empresa C	Comércio	Grande	12000	2300	1%	PCI
Empresa D	Serviços	Grande	15000	7500	Não Informado	Não
Empresa E	Indústria	Grande	1100	700	2%	CVM e Bolsa de Oslo
Empresa F	Indústria	Grande	20000	20000	Menos que 1%	CVM e Lei Sarbanes-Oxley
Empresa G	Serviços	Grande	12000	12000	Menos que 1%	CVM e Basiléia 3
Empresa H	Comércio	Grande	3000	2500	1%	Não
Empresa I	Serviços	Médio	90	90	90%	Não
Empresa J	Serviços	Médio	50	50	90%	ISO 27000
Empresa K	Serviços	Grande	3000	1500	Não Informado	Regulatórios da Rede Nacional de Pesquisas
Empresa L	Serviços	Grande	15000	15000	Menos que 1%	CVM, normas do Banco Central e do Sistema Financeiro Nacional
Empresa M	Indústria	Grande	4000	3200	1%	Não
Empresa N	Indústria	Grande	4500	450	1%	Auditorias Externas Ernst & Young

Fonte: O autor (2014)

Como se pode notar, houve uma predominância de organizações do setor de serviços com sete empresas, seguido pelo setor industrial com cinco empresas e somente duas empresas do setor comercial. Na intenção de pesquisar organizações que lidam frequentemente com Tecnologia e Segurança da Informação, também houve predominância de empresa de grande porte entre as pesquisadas, com 11 observações, e somente três de porte médio, sendo que nenhuma empresa de pequeno porte foi estudada. O número de colaboradores das organizações pesquisadas variou entre 50 e 20000 funcionários, sendo que o número de empregados que utilizam computadores foi relativamente menor e variado entre

as empresas. O percentual do faturamento investido em Tecnologia da Informação dessas empresas variou entre menos que 1% até 90%, sendo que duas organizações não informaram esse valor. Quanto ao valor destoante da realidade atual de 90% de investimento do faturamento das empresas em Tecnologia da Informação observados em dois casos, justifica-se por tratar de organizações que trabalham diretamente envolvidas com Tecnologia da Informação. Em relação aos regulatórios em que as empresas estão sujeitas, verifica-se as auditorias internas e externas, as regras da Comissão de Valores Monetários (CVM), da Bolsa de Oslo (Noruega), da Lei Sarbanes-Oxley (Bolsa de Nova Iorque - EUA), do Banco Central, entre outros. No entanto, foram encontradas cinco organizações que não estão sujeitas a regulatórios.

Quanto à caracterização dos entrevistados, todos os respondentes possuíam o cargo de CIO (*Chief Information Officer*) ou equivalente e eram responsáveis por toda a área de Segurança da Informação da empresa em questão. A seguir, o Quadro 3 mostra a caracterização dos entrevistados.

Quadro 3: Caracterização dos respondentes

Respondentes	Experiência Profissional em TI (em Anos)	Tempo na Atual Função (em Anos)
Gestor A	15	2
Gestor B	10	8
Gestor C	16	2
Gestor D	16	9
Gestor E	30	6
Gestor F	21	4
Gestor G	20	8
Gestor H	18	6
Gestor I	17	2
Gestor J	18	4
Gestor K	8	5
Gestor L	16	3
Gestor M	18	3
Gestor N	7	1

Fonte: O autor (2014)

Em relação aos respondentes, observa-se que a experiência profissional na área de Tecnologia da Informação varia de 7 a 30 anos, sendo que a maioria atua a mais de 15 anos nesse campo. Quanto ao tempo em que os entrevistados desempenham a atual função na

organização em que trabalham, a variação é de um a nove anos, com a maioria cumprindo a função atual a menos de cinco anos.

Nos próximos seis itens, os dados específicos do tema de pesquisa são analisados e interpretados, começando pelo Contexto de Tecnologia e Segurança da Informação e a sua influência no Comportamento Responsável Relativo à Segurança da Informação.

4.2 CONTEXTO DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO E COMPORTAMENTO RESPONSÁVEL RELATIVO À SEGURANÇA DA INFORMAÇÃO

Este item identifica a presença ou não da relação de influência percebida do Contexto de Tecnologia e Segurança da Informação no Comportamento Responsável dos colaboradores relativo à Segurança da Informação, atendendo o primeiro objetivo específico da pesquisa em questão. Como a dimensão Contexto de Tecnologia e Segurança da Informação foi subdividida em duas partes, Entendimento sobre Tecnologia da Informação e Segurança da Informação e Controles e Punições, começaremos pela primeira subdivisão observada. A análise seguirá a ordem das questões apresentadas no roteiro de entrevistas (ver Apêndice A), sendo que cada questão corresponde a uma variável.

A primeira questão a ser analisada diz respeito à variável **Conhecimento e Habilidades**, pertencente à dimensão **Entendimento sobre TI e Segurança da Informação** (subdivisão da dimensão **Contexto de Tecnologia e Segurança da Informação**), e aborda os conhecimentos e as habilidades gerais que os funcionários possuem para proteger os dados da organização. Inicialmente, verificou-se se existe ou não a influência dessa variável no comportamento responsável dos empregados, de acordo com a percepção dos gestores. O Quadro 4 localizado logo abaixo mostra este resultado.

Quadro 4: Influência da variável Conhecimento e Habilidades no Comportamento

Influência Percebida	Frequência
Não	7
Sim	6
Não soube responder	1

Fonte: O autor (2014)

De acordo com a análise dessa questão, apesar da maioria dos gestores responderem que os funcionários **não** possuem conhecimento e habilidades gerais suficientes a ponto de influenciar no comportamento responsável, o resultado final dessa relação não pode ser definitivo, já que a diferença entre os que não observaram e os que observaram a influência

foi mínima. Entretanto, um gestor não soube informar se existe ou não uma relação de influência dessa variável no comportamento dentro da organização a que ele pertence.

Conforme a análise das entrevistas em relação a essa questão, foram consideradas significativas as seguintes categorias: **Familiaridade dos funcionários com Segurança da Informação** e **Programas de capacitação, políticas e certificações suficientes**. A categoria Familiaridade dos funcionários com Segurança da Informação abordou a necessidade dos funcionários em saber lidar com Segurança da Informação para assim saber como se comportar adequadamente frente a vulnerabilidades, o que ficou bastante evidenciado na fala do Gestor B:

> [...] existem profissionais e colaboradores que tem consciência por lidar mais com a informação da empresa no dia a dia, do setor jurídico ou do setor financeiro da empresa, que sabem da importância do sigilo daquelas informações, mas tu vais pegar outras pessoas de outros departamentos, não quer dizer que elas não têm conhecimento da essência daquilo. Elas vão ter, mas seria questão da familiaridade [...]

Em relação à categoria Programas de capacitação, políticas e certificações suficientes, que diz respeito à suficiência com que programas, políticas e certificações devem ou, pelo menos, deveriam fornecer o mínimo necessário para a manutenção de um comportamento responsável em relação à Segurança da Informação, como se pode notar na observação do Gestor I:

> [...] É claro que nós também possuímos, na verdade, outros profissionais, como parte administrativa, como recepcionistas, enfim, que, obviamente, não tem esse *know-how* todo e vêm até com vícios de outras empresas. Nesse caso, o que nós temos daí é a questão da "Academia Energia", que é a área de treinamentos da nossa empresa que é responsável por nivelar, digamos, no padrão mínimo, o discurso de todos da empresa [...]

Logo abaixo, no Quadro 5, encontra-se um resumo com todas as categorias observadas na análise de conteúdo da variável Conhecimento e Habilidades, juntamente com a frequência de vezes com que a mesma foi citada, o total de evidências verificadas e outros exemplos de evidências como forma de caracterização do sentido da categoria criada.

Quadro 5: Categorias da variável Conhecimento e Habilidades

Categorias	Frequência	Total de Evidências	Outras Evidências
Familiaridade dos funcionários com Segurança da Informação	8	9	E4 - [...] claro que isso vai depender do nível de esclarecimento de cada colaborador [...]
Programas de capacitação, políticas e certificações suficientes	7	9	E1 - [...] existem programas de capacitação e políticas que fornecem o mínimo de informações para os funcionários responderem a essa situação [...]
Rotatividade de funcionários como fator negativo na Segurança da Informação	1	2	E1 - [...] os usuários possuem o conhecimento, só que a rotatividade faz com que esse conhecimento vá se perdendo [...]
Pouco caso da empresa com Segurança da Informação	1	2	E2 - [...] a TI só tenta proteger [...]
Pouca maturidade da Segurança da Informação	1	1	E1 - [...] como Segurança da Informação é uma disciplina relativamente nova, não é algo que vem de gerações da vida das pessoas, tanto na vida pessoal quanto na vida profissional, é algo que está em constante evolução, no processo de aumento de maturidade [...]
Necessidade do uso ponderado de recursos de TI pelos colaboradores	1	1	E1 - [...] se eles tiverem uma postura mais comedida, mais ponderada dos recursos tecnológicos, ajuda a diminuir brechas e vulnerabilidades da informação na segurança [...]
Reatividade da área de Segurança da Informação	1	1	E1 - [...] como nós somos reativos na questão de Segurança da Informação, eles ainda são muito carentes de apoio nosso para fazer muitas coisas [...]
Pouca autonomia da área de Segurança da Informação	1	1	E1 - [...] muitas vezes, fazem as coisas sem nos consultar [...]

Fonte: O autor (2014)

A segunda questão trata da variável **Experiência e Conhecimentos Gerais em TI** (Tecnologia da Informação), componente da dimensão **Entendimento sobre TI e Segurança da Informação** (subdivisão da dimensão **Contexto de Tecnologia e Segurança da Informação**), e está relacionada à experiência e ao conhecimento geral do funcionário com Tecnologia da Informação no sentido de tornar seu comportamento adequado à Segurança da Informação. Quanto à existência ou não de influência dessa variável ou não no comportamento responsável, **todos** os entrevistados **confirmaram** que a experiência e o conhecimento geral de Tecnologia da Informação do colaborador influenciam no comportamento responsável relativo à Segurança da Informação, o que traz fortes indícios da confirmação da influência.

Em relação às categorias encontradas na análise de conteúdo dessa variável, temos duas consideradas mais importantes: **Consciência dos funcionários com Segurança da Informação** e **Familiaridade dos funcionários com Tecnologia da Informação**. A categoria Consciência dos funcionários com Segurança da Informação aborda a noção de consciência que o colaborador tem para se comportar de acordo com a necessidade de proteção do ambiente de Segurança da Informação, que pode ser caracterizada pelo trecho da resposta do Gestor F: "[...] dependendo do conhecimento, do interesse que ele tenha e da experiência que ele já tenha feito dentro ou fora da empresa, claro que ele vai ter mais possibilidade de explorar questões de tecnologia [...]".

A categoria Familiaridade dos funcionários com Tecnologia da Informação pondera sobre a necessidade dos colaboradores terem proximidade com Tecnologia da Informação para facilitarem a compreensão do tema e se comportarem adequadamente em relação à Segurança da Informação, semelhante à categoria de familiaridade com Segurança da Informação da variável anterior. Para melhor ilustrar a categoria, o discurso do Gestor N justifica:

> [...] a partir do momento que alguém tem maior familiaridade com Tecnologia da Informação, a tendência é que ela seja mais apta a lidar com a Segurança da Informação. Assim, seu comportamento, provavelmente, será mais consciente e responsável do que os demais, que não têm a vivência com a TI. [...]

A seguir, o Quadro 6 apresenta em resumo todas as categorias encontradas na análise de conteúdo para essa variável.

Quadro 6: Categorias da variável Experiência e Conhecimentos Gerais em TI

Categorias	Frequência	Total de Evidências	Outras Evidências
Consciência dos funcionários com Segurança da Informação	4	4	E3 - [...] a preocupação, até talvez ele tenha, porque, enfim, é inerente [...]
Familiaridade dos funcionários com Tecnologia da Informação	4	4	E2 - [...] todo o funcionário que eu tenho na organização, que conhece a TI ou os níveis de Segurança de TI, ele consegue auxiliar na proteção das suas tarefas, do seu setor, dos dados relativos ao seu trabalho [...] E3 - [...] aquele que não sabe muito, às vezes, por descuido, por falta de conhecimento, acaba trazendo algum problema por manipular de forma inadequada recursos de tecnologia [...]
Necessidade de maturidade dos funcionários com Segurança da Informação	2	2	E2 - [...] eles têm que acompanhar a evolução da tecnologia e de todos os aspectos legais que a empresa possui [...]
Pouco caso dos funcionários com Segurança da Informação	2	2	E1 - [...] o que eu percebo é que pessoas da área de TI tendem a serem mais relaxadas, elas têm a falsa impressão de que sabem como lidar com a Segurança da Informação e, na prática, isso não é verdade [...] E2 - [...] tem o usuário de tecnologia avançado, que tem bastante conhecimento, ele acaba avançando nos níveis de informação que ele pode, muitas vezes até não observando controles de Segurança que existem [...]
Maior cobrança dentro da área de Segurança da Informação	1	2	E1 - [...] eu tenho certeza que em nenhuma outra área os colaboradores são tão cobrados quanto à Segurança da Informação quanto aqui dentro [...]
Pré-qualificação dos funcionários em Segurança da Informação	1	1	E1 - [...] ele tem que passar por um filtro para trabalhar na Segurança da Informação [...]
Bom senso dos funcionários	1	1	E1 - [...] mas o bom senso e o comportamento devem vir acima de tudo [...]
Atitude pró-ativa dos funcionários relativo à Segurança da Informação	1	1	E1 - [...] é fundamental a participação, esse conhecimento de Segurança para que nós tenhamos esse comportamento responsável, porque a tecnologia e o aspecto legal sem o comportamento e a atitude do funcionário, não funcionam [...]

Fonte: Elaborado pelo autor

Em relação à variável **Conhecimento da Política de Segurança da Informação**, item da dimensão **Entendimento sobre TI e Segurança da Informação,** contemplada na terceira questão do roteiro de entrevistas, verifica a influência do conhecimento da Política de

Segurança da Informação e seus efeitos práticos no cotidiano da organização relativo ao comportamento adequado do colaborador frente à Segurança da Informação. Abaixo, o Quadro 7 mostra a relação de influência percebida pelos gestores em relação à variável analisada.

Quadro 7: Influência da variável Conhecimento da Política de Segurança da Informação no Comportamento

Influência Percebida	Frequência
Sim	11
Não	3

Fonte: O autor (2014)

Segundo a avaliação feita pelos entrevistados, a maioria dos gestores (11 casos) respondeu que o conhecimento da política de Segurança da Informação **influencia** no comportamento responsável dos empregados relativo à Segurança da Informação, o que era esperado, conforme a literatura pesquisada, sendo que apenas três gestores negaram essa relação.

Nas principais categorias encontradas na interpretação dos dados da pesquisa em relação à variável analisada, temos: **Exposição da Política de Segurança da Informação**, **Ignorância da política de Segurança da Informação por parte dos colaboradores** e **Política de Segurança da Informação como base para o comportamento**, consecutivamente. A categoria Exposição da Política de Segurança da Informação, que representa a divulgação da Política de Segurança pelas organizações nos mais diferentes meios de comunicação para favorecer a conduta comportamental dos funcionários, teve sete citações, sendo que oito evidências foram verificadas. Duas citações ilustram muito bem a situação, o relato do Gestor E:

> [...] a divulgação da política de Segurança da Informação, com certeza, influencia bastante. Eu pego o exemplo prático lá da empresa onde, cada vez que entra um novo colaborador ou grupo de colaboradores, eu tenho uma reunião com eles durante toda uma manhã onde vou explicar todas as regras de Segurança da Informação para eles. Tem manual, tem guia com a política e cada um dos itens nós vamos exercitar, verificar os pontos e o porquê de cada um deles. Isso leva o colaborador a ter consciência, primeiro da política e, segundo, além de ter consciência, saber as regras e seguir mais facilmente aquele aspecto ou não. [...]

Assim como o relato do Gestor F:

> [...] A divulgação da política e o conhecimento, desde o momento que o funcionário entra na empresa, é fundamental e tem influência no comportamento. Ele sabe que o conhecimento das regras e da base de regras, a regra mínima de Segurança, é importante para orientar o comportamento dele, mesmo que ele decida fugir de uma regra ou não adotar alguma regra. O conhecimento da política é fundamental. [...]

Quanto à categoria identificada como Ignorância da política de Segurança da Informação por parte dos colaboradores, trata-se da pouca importância dada e da falta de motivação dos empregados em conhecer e aplicar os procedimentos da Política de Segurança, que pode trazer implicações no comportamento. A ideia do Gestor D apresenta uma das melhores definições para a categoria: “[...] o ideal seria que todo mundo tivesse, ao menos uma vez toda, durante a história na empresa, lido a política, mas eles não lêem. Quando você entra na empresa, tem um monte de coisa para assinar e o cara não lê [...]”.

Para a terceira categoria mais significativa, chamada de Política de Segurança da Informação como base para o comportamento e que diz respeito ao uso da Política de Segurança como fundamento para toda e qualquer prática ou procedimento que envolva Segurança da Informação, incluindo o comportamento responsável dos colaboradores, pode-se atribuir o seu sentido pela descrição do Gestor I:

> [...] hoje, ainda mais quando nós trazemos para uma cultura latina que é mais permissiva, se não existe uma sanção clara pelo mau uso ou, melhor, se não existe uma definição clara de qual é o uso que se quer da tecnologia, responsável, seguro. Se isso não está bem definido, você não tem nem como classificar, na verdade, que o comportamento não é adequado. E para você poder fazer algum tipo de sanção, controle e, principalmente, para você ter um uso responsável, é preciso você ter a definição. Isso só se consegue através de uma política.

O Quadro 8 apresentado a seguir resume todas as categorias criadas na análise de conteúdo, bem como a frequência, o total de evidências encontradas e outras diferentes evidências também consideradas relevantes.

Quadro 8: Categorias da variável Conhecimento da Política de Segurança da Informação

Categorias	Frequência	Total de Evidências	Outras Evidências
Exposição da política de Segurança da Informação	7	8	E2 - [...] A gente faz periodicamente. Até essa semana teve um e-mail que mandei para a empresa toda sobre a internet, as regras de utilização de e-mails e tudo mais. Então, a questão de ter o acesso e conhecer a política faz diferença [...] E6 - [...] Quando as pessoas entram na empresa, eles assinam um papel dizendo que são responsáveis, estão de acordo com a política e seguindo algumas regras da própria política [...]
Ignorância da política de Segurança da Informação por parte dos colaboradores	4	5	E2 - [...] A questão é: como é que você obriga alguém a ler? Você não obriga ninguém a ler, a pessoa tem que achar que tem que ler, não tem como. Mas quando você vê que as pessoas não leem? Quando você fala que ela não está seguindo, que ela vai ser punida. Aí ela vai lá na política para ver se realmente tem aquilo [...] E3 - [...] Eles não têm interesse, a motivação de ir atrás daquilo, ler e seguir aquilo. [...]
Política de Segurança da Informação como base para o comportamento	3	3	E3 - [...] A política é o alicerce, é a base de toda e qualquer iniciativa, projeto e atividade relacionada à informação e que requeira Segurança. Ela é embasada numa política. Ela que estabelece diretrizes para isso [...]
Consciência dos funcionários com os riscos de Segurança da Informação	2	3	E1 - [...] Se o usuário tivesse consciência. Eu não vou dizer responsabilidade, mas talvez consciência. Fica na consciência mesmo. Eles não têm noção de que um comportamento inadequado pode expor, não só eles, mas também a empresa [...]
Necessidade de aplicação prática da política de Segurança da Informação pelos funcionários	1	1	E1 - [...] é fundamental que todo mundo adapte-se ao modelo de política. Já tivemos casos aqui, principalmente de estagiários, que não fecham com nosso modelo de trabalho e tiveram que ser deslocados para outra área. Então, tem que conhecer a política e aplicar a política [...]
Falta de aplicabilidade da política de Segurança da Informação	1	1	E1 - [...] a gente não tem uma aplicabilidade no dia a dia [...]
Aderência dos funcionários à política de Segurança da Informação	1	1	E1 - [...] tem alguns casos em que a pessoa não sabe como lidar com determinadas situações. Ela tendo conhecimento da política, ela direciona o comportamento dela no sentido de estar mais aderente [...]
Falta de conhecimento sobre Segurança da Informação	1	1	E1 - [...] Hoje, eu responderia isso como não tem influencia porque não existe esse conhecimento de política, dos efeitos e tudo mais [...]

Fonte: O autor (2014)

A pergunta 4 do roteiro de entrevistas, relacionada à variável **Severidade da Política de Segurança da Informação**, parte integrante da dimensão **Entendimento sobre TI e Segurança da Informação**, verifica a relação de influência entre a severidade da Política de Segurança em si com o comportamento apropriado dos empregados em função da Segurança da Informação. Essa relação pode ser comprovada no Quadro 9, localizado abaixo.

Quadro 9: Influência da variável Severidade da Política de Segurança da Informação no Comportamento

Influência Percebida	Frequência
Sim	10
Não	4

Fonte: O autor (2014)

Pelas respostas dos entrevistados na questão 4, é possível observar que a influência da severidade da Política de Segurança no comportamento responsável foi percebida por 10 gestores, o que **corrobora** a relação de influência. Apenas 4 respondentes não conseguiram observar essa relação.

Com relação às categorias constatadas na interpretação das respostas referentes à questão 4, três merecem maior destaque: **Aplicação prática da severidade da política de Segurança da Informação**, **Política de Segurança da Informação como orientação e conscientização** e **Envolvimento de outras áreas na política de Segurança da Informação**. A categoria Aplicação prática da severidade da política de Segurança da Informação, com seis citações, pode ser definida como a verdadeira aplicação da severidade constada na Política de Segurança entre todos os membros da organização sem distinção, o que pode ser verificado pela citação do Gestor I:

> [...] isso está ligado diretamente ao comportamento que ele tem na empresa, porque ele sabe, e não só porque está escrito, mas porque, na prática, se implementa essa política. Não é só uma política que está somente escrita. Nós já tivemos casos de desligamento e tudo mais. Então, a política e o exemplo fazem com que o profissional, ele sim tenha um comportamento mais aderente à nossa política que o mercado, por exemplo, que das empresas comuns que não utilizam, que nem política tem [...]

A passagem descrita pelo Gestor M também confirma a aplicação prática da severidade da Política de Segurança como um fator importante para determinar o comportamento do funcionário:

> [...] E eu não tenho dúvida que, nas empresas onde, não onde está escrito, porque uma coisa é a empresa ter a possibilidade de penalizar algum colaborador com base no que está escrito, outra coisa é, efetivamente, penalizar. As empresas que,

> efetivamente, penalizam, eu não tenho dúvida que o colaborador é mais cauteloso. [...]

Como a segunda categoria mais citada, com cinco citações e seis evidências verificadas, a Política de Segurança da Informação como orientação e conscientização indica a Polícia de Segurança como uma das principais formas de orientar e conscientizar os colaboradores para manter um comportamento relativamente seguro frente à Segurança da Informação. Uma das principais citações e que melhor caracteriza essa categoria pode ser a descrita pelo Gestor N, que não considera a severidade da Política o aspecto mais significativo para o comportamento responsável:

> [...] A severidade pode influenciar no comportamento, mas ela não é a única coisa que pode fazer isso. A orientação e a conscientização também são boas maneiras para moldar o comportamento. Mostrar para os funcionários o motivo dessas regras de Segurança, o investimento que foi feito, ou seja, conscientizá-los da necessidade de regras e normas de Segurança da Informação. Creio que a severidade e a punição não são o melhor caminho. [...]

A categoria Envolvimento de outras áreas na política de Segurança da Informação, terceira mais citada com cinco observações, aborda a participação de outras áreas da organização para desenvolver, manter, apoiar, punir, entre outras atividades relacionadas à Política de Segurança da Informação. Diversas áreas foram citadas nessa categoria, tais como a jurídica (no sentido de fornecer subsídios para formular as punições de acordo com as normas trabalhistas), o Recursos Humanos – RH (com a função de definir e formalizar a punição) e outros setores específicos (quando o gestor direto do colaborador que violou alguma norma de Segurança tem a responsabilidade de definir a forma de punição a ser empregada). A visão do Gestor F pode servir como ilustração dessa situação:

> [...] O que tem severidade depois é o não cumprimento em relação à política, trazendo então, até, em último caso, penalidades que podem ser colocadas para os funcionários, pelo setor de Recursos Humanos ou pelos gestores dos responsáveis, se ele não cumprir ou deixar de observar alguma dessas regras. [...]

O Quadro 10, apresentado na sequência, resume todas as categorias encontradas nesta variável, bem como outras evidências, justificando todas as delimitações.

Quadro 10: Categorias da variável Severidade da Política de Segurança da Informação

Categorias	Frequência	Total de Evidências	Outras Evidências
Aplicação prática da severidade da política de Segurança da Informação	6	6	E1 - [...] quando aplicada essa severidade sim, porque as vezes é só no papel e ninguém leva a sério. [...] E2 - [...] Então, eventualmente, a gente está demitindo, aplicando advertências formais. Está tudo dentro da política e o pessoal sabe que vai ser mesmo. Claro, a gente não consegue pegar todo mundo, mas tu sabes que quando for pego, a coisa vai a nível de diretoria e ninguém passa a mão na cabeça de ninguém. [...]
Política de Segurança da Informação como orientação e conscientização	5	6	E3 - [...] no meu entendimento uma política não deve ser apenas punitiva, ela tem que deixar claro o que pode e o que não pode. E não a penalidade que a pessoa vai sofrer. [...]
Envolvimento de outras áreas na política de Segurança da Informação	5	5	E1 - [...] Na política, hoje, a gente tem como três advertências. É justamente por isso que tem que envolver a parte jurídica no tipo de punição. [...] E3 - [...] Então, ela é severa, mas não é punitiva. Quem pune é o RH da empresa [...]
Aspectos culturais influenciando na severidade da política de Segurança da Informação	2	2	E1 - [...] No Brasil, a gente tem uma política, tem uma cultura de impunidade. O cara bebe um monte, atropela meia dúzia e no outro dia sai. Paga a pena e sai. A questão da impunidade é inerente ao nosso dia a dia. Então assim, tu consegues diminuir um certo tipo de crime ou um certo tipo de delito quando tu aplicas uma punição ou penalidade muito alta, uma multa muito alta, para a pessoa saber que se for pega, vai dar problema. Então é isso, quanto mais severa é a política, mais o pessoal vai pensar duas vezes antes de tentar burlar. [...]
Aversão dos funcionários à severidade da política de Segurança da Informação	2	2	E1 - [...] o pessoal tende a não querer seguir a política em função dela ser muito restritiva, dela ser muito severa nesse sentido [...]
Pouco caso da empresa com Segurança da Informação	1	2	E2 - [...] eu acho que isso deveria ser reforçado na nossa empresa ainda, nós ainda estamos num trabalho muito no início e essa severidade tem que ser muito melhorada para chegar naquilo que nós da TI desejamos. [...]
Exposição da severidade na política de Segurança da Informação	1	2	E1 - [...] Ela tem que estar explícita dentro da política [...]
Incidentes de Segurança da Informação pouco determinantes em demissões	1	1	E1 - [...] Literalmente, você usa outras coisas, não só isso para demitir a pessoa [...]
Manutenção ou reativação da política de Segurança da Informação	1	1	E1 - [...] É um processo gradual e reciclável. Você tem uma empresa desse tamanho, você vai ter que manter não só a política fresca na memória das pessoas que já estão aqui, quanto nas que estão entrando. [...]
Política de Segurança da Informação muito ligada a questões técnicas	1	1	E1 - [...] Nós ainda temos a parte de políticas muito associadas às questões puramente técnicas e isso, na prática, impede que as empresas tomem uma ação num caso efetivo de problema relativo à Segurança. [...]

Fonte: O autor (2014)

Com a conclusão da análise da quarta questão, referente a quarta variável, encerra-se a análise individual dos componentes integrantes da subdivisão Entendimento sobre TI e Segurança da Informação. Na conclusão deste item, será retomada a análise a partir de uma visão holística, englobando as duas subdivisões da dimensão Contexto de Tecnologia e Segurança da Informação.

Partindo para a análise de conteúdo individual das variáveis pertencentes à dimensão **Controles e Punições** (a outra subdivisão da dimensão **Contexto de Tecnologia e Segurança da Informação**), temos a quinta questão, referente à variável **Mecanismos de Controle como Inibidores do Desempenho e da Criatividade**. Esta variável se refere aos controles utilizados na Segurança da Informação como forma de inibir a capacidade de desempenho e bloquear a criatividade dos colaboradores a ponto de influenciar no comportamento responsável relativo à Segurança da Informação. Quanto à existência ou não da influência percebida pelos respondentes na variável, não foi possível confirmar essa relação, pois houve uma igualdade entre as respostas dos gestores (sete afirmações e sete negações). Logo, essa relação de influência foi considerada **inconclusiva**.

Como as categorias mais importantes encontradas na análise dessa variável, temos: **Políticas e mecanismos de controle de Segurança da Informação diferenciados para cada ambiente/setor específico**, **Equilíbrio entre a necessidade do negócio/atividade e a tecnologia** e **Criação e avaliação da política e dos mecanismos de controle de Segurança da Informação**. A categoria Políticas e mecanismos de controle de Segurança da Informação diferenciados para cada ambiente/setor específico, que obteve seis citações entre as 14 entrevistas, pode ser determinada como uma particularidade da Política ou dos controles, que devem ser atribuídos conforme as especificidades e as necessidades de cada ambiente ou setor. Com relação a diferentes ambientes, o Gestor I faz a seguinte consideração:

> [...] aplicar uma política que vale, por exemplo, para uma empresa que é um grupo de Segurança da Informação, e aplicar essa mesma política para um escritório de advocacia e para uma agência de publicidade, vai ter, com certeza, um resultado diferente em cada um dos ambientes. E, possivelmente, no caso, falando da nossa política, numa agência de publicidade, a agência de publicidade iria falir, porque ela não iria conseguir acessar a rede social e outras tantas coisas que ela precisaria para a execução do trabalho. [...]

Na diversificação da Política e dos controles por setores em uma mesma organização, o gestor H diz:

> [...] Marketing tem acesso à Facebook, Twitter, redes sociais, assim como o setor de compras também, para acompanhar todo o mercado, toda a parte de evolução do

> mercado. Conforme a área, é controlado, com documento, com termo, com ciência do responsável direto. Assim que ocorre aqui dentro. [...]

A segunda categoria mais citada teve quatro observações, porém com oito evidências registradas. Sendo chamada de Equilíbrio entre a necessidade do negócio/atividade e a tecnologia, ela diz respeito à necessidade de uma Política de Segurança balanceada entre os processos de negócio ou as atividades fins da organização e a tecnologia disponível para o desempenho pleno das funções na empresa. A descrição feita pelo Gestor I caracteriza bem a categoria:

> [...] Não existe receita de bolo para a política, a política é construída com base no negócio e não com base só na tecnologia. Então, você não pode dizer, por exemplo, que Facebook é nocivo ou não é nocivo sem fazer o contraponto com o negócio. É o negócio que determina se aquela tecnologia é interessante ou não para ser utilizada, liberada. [...]

O Gestor L também faz essa mesma relação, frisando que a informação necessita estar disponível para quem precisa dela:

> [...] Enfim, quem tem acesso a determinado tipo de informação é quem, efetivamente, precisa dessa informação para trabalhar dentro da instituição. Do contrário, não. É aquele conceito básico de Segurança da Informação de *need to know*, aquilo que, efetivamente, você precisa saber para executar as suas atividades. [...]

A terceira categoria considerada mais relevante foi a Criação e avaliação da política e dos mecanismos de controle de Segurança da Informação, com quatro citações e cinco evidências descobertas. Trata-se da necessidade de abordar os itens que realmente precisam ser tratados na Política de Segurança ou controlados pelos mecanismos vigentes durante sua criação e em posteriores revisões periódicas, no sentido de não inibir o funcionário. Isto pode ser ilustrado pela fala do Gestor N: “[...] Onde houver um impasse entre a gestão dos processos de negócio e a gestão da Segurança de Informação, a política e os mecanismos de controle devem ser reavaliados [...]”. Na sequência, o Quadro 11 mostra um resumo de todas as categorias atribuídas, bem como outras ilustrações de evidências encontradas.

Quadro 11: Categorias da variável Mecanismos de Controle como Inibidores do Desempenho e da Criatividade

Categorias	Frequência	Total de Evidências	Outras Evidências
Políticas e mecanismos de controle de Segurança da Informação diferenciados para cada ambiente/setor específico	6	6	E6 - [...] tem coisas como uma rede social, por exemplo, que não tem nada a ver com uma área de infra, com uma área de Segurança da Informação, com um área de desenvolvimento de sistemas, mas tem a ver com uma área, por exemplo, de comunicação institucional, com uma área de marketing, e nós somos permissivos nesse sentido. [...]
Equilíbrio entre a necessidade do negócio/atividade e a tecnologia	4	8	E2 - [...] A questão é o equilíbrio. O ponto de equilíbrio cada setor, cada negócio vai ter o seu. [...] E8 - [...] todas as ferramentas necessárias para o pleno desempenho das atividades do funcionário devem ser fornecidas. [...]
Criação e avaliação da política e dos mecanismos de controle de Segurança da Informação	4	5	E4 - [...] Então, ela está relacionada sim à inibição, mas, na verdade, ela só inibe quando ela é mal construída. [...]
Restrição de acesso geral devido a alguns funcionários	3	4	E2 - [...] No momento em que você é obrigado a fazer uma internet altamente restrita em função de mau uso de um, você impede que o outro, que quer fazer uso para o bem, tenha pouco acesso porque a internet ficou tão bloqueada que nenhum site adequado, digamos assim, consegue ser acessado. [...]
Flexibidade da política e dos mecanismos de controle de Segurança da Informação	3	3	E2 - [...] Nós, aqui dentro, hoje em dia, eu consigo te dizer que não, isso está muito flexível. As ferramentas de Segurança não estão inibindo eles. Eles têm um caminho a seguir, eles assinam alguns termos dizendo que se responsabilizam pelos acessos e os acessos são concedidos. [...] E3 - [...] Se o mecanismo está relacionado com a inibição, sim. Ele pode estar relacionado. Mas na verdade, o determinante é o quão flexível a tua política de Segurança é na prática. [...]
Necessidade dos mecanismos de controle de Segurança da Informação	2	2	E1 - [...] eu entendo que isso é necessário mas acho que em alguns casos onera bastante o desempenho. [...] E2 - [...] mas isso é uma regra, uma forma de você preservar o conjunto, da empresa como um todo se preservar contra os riscos que poderiam estar expostos.
Gestores como limitadores dos mecanismos de controle de Segurança da Informação	2	3	E2 - [...] Se o diretor que é responsável daquela pessoa disser que ele não precisa, então não foi diretamente a política de Segurança que barrou ele. A política de Segurança é permissiva nesse sentido, o que barrou foi o gestor direto dele. [...]
Mecanismos de controle de Segurança da Informação como orientadores	1	1	E1 - [...] Nós trabalhamos muito no sentido de influenciar e dar chance ao pessoal, não só da Segurança, mas geral da empresa, de desempenhar sua criatividade toda e a política busca, os controles buscam, simplesmente, fazer uma orientação [...]
Política de Segurança da Informação como condicionadora de comportamento	1	1	E1 - [...] Porque a política diz que tem que ser daquela forma, então ela tende a seguir daquela forma e acaba inibindo assim, às vezes. Poderia, de repente, se achar uma solução bem mais interessante para algum problema e o pessoal acaba assim. Se a política não permite, então eu não vou nem tentar. [...]
Comparação do ambiente organizacional com outros ambientes menos controlados	1	1	E1 - [...] o ambiente dentro de uma empresa é totalmente diferente do ambiente doméstico ou mesmo da universidade, que se tem muito mais liberdade. Então, muitas pessoas enxergam isso realmente como restrição de criatividade e desempenho porque ele não pode fazer tudo o que ele faz em casa dentro de uma empresa [...]

Fonte: O autor (2014)

Quanto à sexta questão, referente à variável **Mecanismos de Controle da Violação de Regras e Normas**, integrante da dimensão **Controles e Punições** (subdivisão da dimensão **Contexto de Tecnologia e Segurança da Informação**), podemos dizer que ela aborda as maneiras com que a organização controla a violação de regras e normas de Segurança da Informação pelos colaboradores, o que também inclui controles de reincidência, e sua incidência no comportamento responsável. No Quadro 12, é mostrada a relação de influência percebida pelos entrevistados.

Quadro 12: Influência da variável Mecanismos de Controle da Violação de Regras e Normas no Comportamento

Influência Percebida	Frequência
Não	10
Sim	4

Fonte: O autor (2014)

Como se pode observar pelas respostas dos gestores, **não** foi percebida influência dos controles de violação de regras e normas no comportamento responsável dos empregados (10 respostas negativas), com apenas quatro entrevistados tendo respostas positivas.

Em relação à interpretação categorial da questão 6, foram observadas quatro categorias consideradas mais significativas, respectivamente: **Punição diferenciada de acordo com cada caso**, **TI sem autonomia para aplicar punições**, **TI com a função de reportar incidentes de Segurança da Informação** e **Política de Segurança da Informação como norteadora das ações em casos de incidentes**. A categoria mais citada, que obteve nove observações e 14 evidências encontradas, chama-se Punição diferenciada de acordo com cada caso e foi assim denominada por tratar das diferentes punições atribuídas pelas organizações conforme os mais diferentes critérios, entre eles, a gravidade do incidente, a reincidência, a índole do colaborador, a intenção do funcionário e os riscos envolvidos. O conteúdo apresentado pelo Gestor L exemplifica bem essa situação:

> [...] cada caso é analisado isoladamente. Se o colaborador se apropriou indevidamente de informação para efetuar uma fraude, por exemplo, o que acontece em toda e qualquer empresa, de toda e qualquer natureza, acontece num banco, numa padaria, numa universidade, toda e qualquer empresa que está atrelada ao comportamento humano, que são todas. Não existe empresa só de robôs. Ela está suscetível a ter problemas relacionados a fraudes. Então, se nós temos algum problema dessa natureza, o direcionamento da punição, da sanção, é um. Se é um outro tipo de problema relacionado à Segurança como, por exemplo, a pessoa acessar um site de conteúdo impróprio na internet que não deveria, é um outro tipo de ação. Se a pessoa acessar um site impróprio durante 5 minutos, talvez não seja um evento tão grave. Mas se a pessoa é reincidente, constantemente tem tentado burlar mecanismos de Segurança para acessar, por exemplo, um site de conteúdo erótico, um site de conteúdo fraudulento, então se tem um tipo de ação. [...]

A ideia apresentada pelo Gestor D também serve como ilustração da diversidade dessa categoria:

> [...] Claro que tem alguns casos que são críticos, por exemplo, o cara tentando mandar vídeos pornográficos para um cliente, isso não tem dúvida que é desperdício de banda de internet. Mas um caso onde tinha uma mulher que estava mandando fotos do aniversario da filha para outro endereço, aí tu vai lá e fala. Tem uma questão de bom senso. [...]

A categoria TI sem autonomia para aplicar punições apresentou cinco observações e sete evidências. Ela diz respeito à falta de autonomia da área de Tecnologia ou de Segurança de Informação em aplicar a punição definida na Política de Segurança, o que pode ser verificado na frase do Gestor J:

> [...] normalmente nós envolvemos a equipe de RH nisso, porque, às vezes, tem questões jurídicas, questões de legislação trabalhista. Então, nós sempre envolvemos o RH. E o RH sempre se demonstra assim, muito receoso de colocar um limite muito grande em função disso e tal, de definir alguma questão de punição [...]

Em relação à categoria TI com a função de reportar incidentes de Segurança da Informação, que teve cinco citações e evidências, ela pode ser caracterizada pelo uso das áreas de Tecnologia ou Segurança da Informação com a principal função de reportar incidentes de Segurança para outras áreas ou responsáveis, o que pode se notado na fala do Gestor N: “[...] O que nós fazemos quando um funcionário viola as regras, quando acontece algum incidente, é reportar o fato para a gerência da pessoa que cometeu o incidente [...]”.

A última categoria melhor avaliada foi Política de Segurança da Informação como norteadora das ações em casos de incidentes, que obteve as mesmas qualificações da categoria anterior. Abordando a Política de Segurança como a base fundamental para qualquer ação em casos de eventos de Segurança da Informação, essa categoria pode ser evidenciada nos dizeres do Gestor L: “[...] Na política está estabelecido quais as possíveis sanções para comportamentos inadequados no que diz respeito à Segurança da Informação [...]”.

A seguir, no Quadro 13, encontra-se o resumo de todas as categorias verificadas, a frequência de observações, o total de evidências e outros exemplos para caracterização das categorias.

Quadro 13: Categorias da variável Mecanismos de Controle da Violação de Regras e Normas

Categorias	Frequência	Total de Evidências	Outras Evidências
Punição diferenciada de acordo com cada caso	9	13	E2 - [...] Que tipo de punição? Bom, depende, depende da gravidade do ocorrido, pode ser uma notificação, pode ser advertência, pode ser um desligamento, aí não sei, depende [...] E7 - [...] vão avaliar o caso, que pode ser uma punição de suspensão do funcionário até demissão por justa causa [...] E11 - [...] decidir qual a forma de reeducar o usuário ou até aplicar uma sanção pelo fato dele ter violado a regra. Isso é uma decisão posterior, conforme o caso [...]
TI sem autonomia para aplicar punições	5	7	E1 - [...] a TI não tem autonomia para aplicar advertência, quem aplica advertências é o RH. [...] E10 - [...] eu não controlo qual é a punição [...] E14 - [...] vai conversar com o gestor direto e esse gestor é quem vai tomar uma providência. [...]
TI com a função de reportar incidentes de Segurança da Informação	5	5	E1 - [...] se ela for identificada, o papel da TI é fazer o dedo duro: "Olha, foi identificado, isso foi causado pelo fulano de tal". [...]
Política de Segurança da Informação como norteadora das ações em casos de incidentes	5	5	E2 - [...] Na verdade, a empresa toma as ações cabíveis dentro da política de Segurança da Informação [...] E4 - [...] normalmente, nós orientamos que seja definido um critério assim e até, se possível, na própria política [...]
Registro das ações internas como forma de controle	4	4	E4 - [...] É que a advertência formal fica arquivada. Então, isso pesa [...]
Orientação e conscientização pontuais no lugar de punição	3	7	E2 - [...] hoje, o que a gente faz quando alguém viola uma regra é instruir. Treinar e instruir pontualmente. Ou eu ou outro responsável ou as pessoas que estão envolvidas entram em contato com aquela pessoa e tentam entender a situação justamente para não ocorrer nada mais naquele sentido [...] E7 - [...] existem orientações nesse sentido, mas aí não é aplicada uma punição, são reuniões de orientação que nós temos, educacionais mesmo [...]
Punição como orientação básica em casos de incidentes de Segurança da Informação	2	3	E1 - [...] a orientação básica é punição. A princípio, é punição. [...]
Falta de aplicação prática das punições e da política de Segurança da Informação	2	3	E2 - [...] não se segue o que está escrito na norma. Penalidade 1, penalidade 2, até justa causa ou algo do gênero. Não, isso não é seguido [...]
Falta de definição e formalização das punições	2	2	E1 - [...] Essa que é a grande questão, não tenha nada escrito assim: 'olha, se fizer isso vai ser punido ou vai ser desligado da empresa'. [...]
Necessidade dos controles de Segurança da Informação	1	2	E1 - [...] esses controles devem estar desenhados para perceber que isso aconteceu. [...]

Fonte: O autor (2014)

A pergunta 7 do roteiro de entrevistas versa sobre a variável **Punição como Inibidor da Reincidência de Eventos de Segurança da Informação**, da dimensão **Controles e Punições**, e considera a punição uma forma de evitar a reincidência de erros ou violações dos

funcionários, a ponto de influenciar no comportamento responsável destes. A relação de influência percebida pelos entrevistados pode ser vista no Quadro 14.

Quadro 14: Influência da variável Punição como Inibidor da Reincidência de Eventos de Segurança da Informação no Comportamento

Influência Percebida	Frequência
Sim	11
Não	3

Fonte: O autor (2014)

Com 11 afirmações, foi possível identificar **uma relação de influência** percebida pelos entrevistados da punição como inibidora da reincidência de incidentes de Segurança da Informação no comportamento responsável dos colaboradores.

Quanto às categorias identificadas na análise dessa questão, as mais significativas foram: **Punição como exemplo para orientar e conscientizar os funcionários** e **Orientação e conscientização ao invés da punição**. Com 10 verificações e evidências, a categoria Punição como exemplo para orientar e conscientizar os funcionários foi a mais citada. Essa categoria caracteriza a punição como maneira exemplar que serve de modelo para orientação e motivo de conscientização para os colaboradores, observações que podem ser notadas no relato do Gestor F:

> [...] Em casos quando existe uma punição justa para algum ato que uma pessoa ou alguém fez contrariando políticas da empresa, nem só política de Segurança da Informação, isso tem um efeito sobre a pessoa, porque ela vai refletir nisso e da importância, que as regras que estão lá não são somente orientações, são regras importantes que garantem que a empresa preserve a estabilidade dela. Além disso, a punição influencia o meio, porque as pessoas também vêem isso como um exemplo que as regras realmente são feitas para serem seguidas. Então ela tem um comportamento sobre a pessoa e tem um comportamento sobre outras pessoas que estão observando essa situação. [...]

A descrição do Gestor M também representa adequadamente a categoria criada:

> [...] a partir do momento que há uma penalização, aquilo serve de exemplo e sempre influencia os demais colaboradores. Porque, a partir do momento, vou citar outro exemplo, está escrito na política que você não pode trabalhar com HD externo. A partir do momento que você detecta que isso aconteceu e que você penaliza esse colaborador, o colega do lado dele ou do andar de cima vai saber que ele foi penalizado e não vai ter aquele tipo de comportamento. [...]

Em relação à categoria denominada Orientação e conscientização ao invés da punição, houve três citações e cinco evidências encontradas. Ela pode ser definida como o uso primordial de meios para orientar e conscientizar os colaboradores em alternativa à punição direta, verificado na passagem contada pelo Gestor E:

> [...] Agora, no nosso entendimento, lá dentro da nossa empresa, primeiro a conscientização. Outra coisa, sempre se dá o entender da pessoa, porque fez aquele ato. Então, se dá à forma de dialogo. Agora, a punição simples, sem ter uma consciência, não é feito dentro da minha organização, onde eu trabalho. [...]

Todas as categorias vistas e outros relatos considerados interessantes para a análise dessa variável estão resumidos no Quadro 15, disponível logo a seguir.

Quadro 15: Categorias da variável Punição como Inibidor da Reincidência de Eventos de Segurança da Informação

Categorias	Frequência	Total de Evidências	Outras Evidências
Punição como exemplo para orientar e conscientizar os funcionários	10	10	E3 - [...] alguns desses notificados ajuda a fazer com que o pessoal use, principalmente, de forma mais comedida: 'o fulano de tal estava usando tal coisa e acabou sendo demitido'. O pessoal fica um pouco mais com um pé atrás [...] E7 - [...] Sem dúvida. A partir do momento que alguém comete uma infração e essa pessoa sofre algum tipo de sanção, de responsabilidade sobre a infração que ela cometeu, invariavelmente, outras pessoas ficam sabendo. Isso serve, sim, como exemplo [...]
Orientação e conscientização ao invés da punição	3	5	E2 - [...] a conscientização é mais forte que a punição [...] E5 - [...] uma advertência ou uma chamada de atenção também resolve, já que ela pode orientar e conscientizar de uma forma mais branda. [...]
Necessidade da aplicação prática das punições	2	2	E1 - [...] Se você cria uma regra e você formaliza que não vai ser feito e se fosse feito a pessoa vai ser punida e, quando acontece, você não pune, o que se vai pensar? Essa regra aí é para inglês ver. Então, se precisar fazer, eu vou fazer [...]
Tempo limitado da inibição da reincidência provocada pela punição	1	1	E1 - [...] Para a pessoa que foi advertida funciona mais tempo. Para os que estão ao redor, funciona de duas a três semanas, no máximo. [...]
Punição pouco severa para inibir a reincidência	1	1	E1 - [...] Ela não consegue inibir porque, justamente, não é muito severa a punição. [...]
Punição como inibidora da reincidência em incidentes de Segurança da Informação mais graves	1	1	E1 - [...] A punição pode também inibir a reincidência, mas isso seria em casos mais graves, em incidentes mais graves. [...]

Fonte: O autor (2014)

A variável **Monitoramento**, relativa à questão 8 e componente da dimensão **Controles e Punições**, aborda a ação de monitoramento das atividades dos colaboradores e sua influência no comportamento adequado em relação à Segurança da Informação. No Quadro 16, observa-se a relação de influência percebida nesta variável.

Quadro 16: Influência da variável Monitoramento no Comportamento

Influência Percebida	Frequência
Sim	13
Não	1

Fonte: O autor (2014)

Conforme se pode notar, basicamente todos os respondentes confirmaram o monitoramento como um fator influenciador do comportamento responsável dos empregados, exceto um único entrevistado, que negou perceber essa influência.

Seguindo para as categorias mais relevantes dessa variável, foi possível apontar estas: **Monitoramento constante para posterior verificação** e **Relação do monitoramento e da restrição de acesso em ambientes diferenciados**. A categoria Monitoramento constante para posterior verificação está relacionada com o monitoramento em tempo integral, porém sem análise imediata desses dados, todos os registros considerados importantes para a organização ficam gravados para uma eventual verificação futura, caso seja necessário. Essa categoria obteve 10 observações e 15 evidências encontradas, que pode ser caracterizada pela explicação do Gestor L:

> [...] é humanamente impossível você estabelecer um processo de monitoramento, um processo de monitoramento online, mas toda e qualquer informação é passível de monitoramento. Eu posso resgatar isso a qualquer tempo, mas não é monitorado, na sua essência. Mas, se for necessário, vai estar lá registrado, tem eventos de auditoria que eu posso ir lá e resgatar um e-mail que o colaborador enviou, um site que ele acessou, um acesso no sistema. [...]

O discurso do Gestor K também pode servir como complementação dessa abordagem:

> [...] Na verdade, tem aquela questão. Todo o e-mail interno de qualquer empresa, o administrador de correio pode ir lá e ler, só que ele não tem tempo. Mas se o coordenador, o diretor disser que quer ver os e-mails que ele está trocando com as pessoas, é possível ir lá e fazer isso. [...]

A outra categoria com melhor avaliação, Relação do monitoramento e da restrição de acesso em ambientes diferenciados, teve quatro citações e está relacionada com o monitoramento e os bloqueios de acesso diferentes em ambientes ou setores diferenciados. O parágrafo do comentário do Gestor L ilustra essa situação:

> [...] Alguns sistemas são restritos, uns são integrados com a rede, outros não. A liberação da internet é mais no grande volume, existem categorias de sites que não são liberados, por exemplo, webmails particulares são bloqueados, mídias sociais são liberadas somente para áreas de comunicação e marketing, para áreas de atendimento, call center, só tem acesso a sites de trabalho, site da empresa, sites de bancos, receita federal, coisas do gênero. Um fato interessante é que as áreas de comunicação e marketing têm mais acessos liberados e podem mandar e-mails maiores que o presidente. [...]

No Quadro 17, localizado abaixo, são apresentadas todas as categorias descoberta, assim como a frequência de observações, o total de evidências encontradas e outras evidências para apreciação.

Quadro 17: Categorias da variável Monitoramento

Categorias	Frequência	Total de Evidências	Outras Evidências
Monitoramento constante para posterior verificação	10	15	E5 - [...] O que eu sei é que, na política, ela diz que pode monitorar a qualquer momento. Então, se precisar monitorar, a empresa tem os recursos. Provavelmente, o que deve acontecer é armazenar o registro disso tudo, mas só é monitorado em casos que seja necessário fazer algum tipo de investigação. [...] E15 - [...] Todos os funcionários têm um login e uma senha de rede para logar em suas máquinas. A partir desse login, é monitorado todo o acesso dos funcionários à internet e aos sistemas de trabalho disponíveis. Todos os registros das máquinas são gravados e, caso haja necessidade, são verificados e analisados, pois não temos condições de monitorar tudo em tempo real. [...]
Relação do monitoramento em ambientes diferenciados	4	4	E3 - [...] Os acessos à internet podem ser diferenciados. Dependendo do setor, têm setores que tem mais liberdade, que foram solicitados. E até de serviços. Tem certas unidades que são super bloqueados, que foi solicitado que não fosse possível acessar nada na internet, pois há informações extremamente sigilosas. Outras não precisam desse sigilo, são mais para serem usados mesmo os serviços da internet. [...]
Aviso prévio de monitoramento	2	2	E2 - [...] a empresa faz o monitoramento avisando o funcionário sempre que faz antecipadamente, isso é uma das primeiras regras, um dos primeiros contratos estabelecidos com o funcionário, e então fica fazendo parte da regra do relacionamento profissional. [...]
Monitoramento por questões de produtividade dos colaboradores	2	2	E1 - [...] A maioria das empresas tem, elas costumam monitorar. Talvez não por questões de confidencialidade e coisas desse tipo. Eu vejo mais por questão de produtividade. [...]
Responsabilidade dos funcionários com a Segurança da Informação	2	2	E1 - [...] Em relação ao acesso dos funcionários aos computadores da empresa, assim como dentro de qualquer empresa, o princípio básico é o do login pessoal e que a pessoa é responsável por aquilo assim como é responsável pela chave da casa dela. Então, todos os acessos feitos com o login de uma pessoa é responsabilidade dela [...]
Monitoramento como forma de orientação	1	1	E1 - [...] Tudo isso é controlado e nós usamos sim essa informação para advertir, para orientar, principalmente para orientar, porque a situação é bem educativa, via de regra, nesses casos. [...]
Segurança da Informação atuando de forma reativa	1	1	E1 - [...] Hoje, nós trabalhamos de forma reativa e atuamos só quando ocorre algum evento onde nós somos chamados para tentar identificar o que ocorreu. [...]
Monitoramento em tempo real	1	1	E1 - [...] nós temos monitoramento de links e monitoramento de alguns processos de negócio, nós temos alerta para tudo isso e, dependendo da criticidade, o alerta via sms não é só durante o horário comercial, ele é também 24 horas por 7 dias da semana. [...]

Fonte: O autor (2014)

A questão 9, correspondente à última variável da dimensão **Controles e Punições**, denominada **Monitoramento como Inibidor de Eventos de Segurança da Informação**, diz respeito ao monitoramento consciente feito pela organização na intenção de inibir, coagir ou acuar os colaboradores e evitar incidentes de Segurança da Informação, implicando no comportamento responsável destes. A relação de influência percebida pelos gestores nesta variável está apresentada no Quadro 18.

Quadro 18: Influência da variável Monitoramento como Inibidor de Eventos de Segurança da Informação no Comportamento

Influência Percebida	Frequência
Sim	11
Não	3

Fonte: O autor

Como a maioria das respostas dos entrevistados foi positiva (11 casos), é possível afirmar que foram encontrados **fortes indícios da influência** do monitoramento usado para fins de inibição de incidentes de Segurança no comportamento adequado dos colaboradores, até porque somente três gestores tiveram resposta negativa.

Com relação às categorias melhor classificadas descobertas nesta variável, temos as seguintes: **Monitoramento consciente como orientador do comportamento** e **Dependência da percepção dos funcionários na inibição causada pelo monitoramento**. Monitoramento consciente como orientador do comportamento, categoria melhor qualificada com 13 observações e também 13 evidências, aborda o monitoramento consciente realizado pelas organizações com a intenção de orientar e moldar o comportamento dos colaboradores, o que pode ser justificado na passagem descrita pelo Gestor F:

> [...] quando existe monitoramento, que os desvios são realmente tratados, as pessoas percebem que realmente existe controle, elas tem uma atitude diferente do que tomar qualquer ação até contrária à política e perceber que não tem nenhuma consequência. Essas questões também vão virando até uma cultura, com as pessoas comentando entre elas. Quando existe qualquer tipo de controle, o monitoramento é uma das formas em alguns casos, isso é claro que influencia, já que as pessoas sabem que existe uma preocupação da empresa com essas questões. [...]

O Gestor J complementa dizendo que o monitoramento pode levar a uma possível punição, o que também serve de orientação:

> [...] Eu acredito que sim porque, na verdade, o monitoramento vai levar à punição e ninguém quer ser punido ou quer ser lembrado por algum prejuízo por causa da empresa, mesmo que esse prejuízo não seja financeiro, pode ser um prejuízo de imagem dele, prejuízo de imagem da empresa ou de uma área. Então, eu diria que

> sim. Se ela souber que está sendo monitorada, ela tende a seguir mais a política e ter um comportamento mais responsável. [...]

Sintetizando toda a ideia apresentada nesta categoria, temos a exposição do relato do Gestor N:

> [...] A verdade é que o monitoramento, quando é divulgado e exposto de forma direta e clara pela empresa, tende a contribuir para o comportamento responsável. De maneira geral, funcionários, quando sabem que estão sendo monitorados, tomam mais cuidado com relação à Segurança da Informação e irão pensar duas vezes antes de quebrar uma regra de Segurança. [...]

A segunda categoria mais citada, Dependência da percepção dos funcionários na inibição causada pelo monitoramento, teve duas citações e três evidências encontradas. Ela trata da relação de dependência da percepção de cada colaborador em particular para enfim provocar inibição ou não no comportamento dele a partir do monitoramento, fator identificado na descrição apresentada pelo Gestor A:

> [...] Acho que isso depende muito do colaborador, de funcionário para funcionário, mas, de certa forma, eu acho que o monitoramento consciente, em alguns, vai inibir, outros vão se sentir coagidos e outros vão se sentir acuados. Então, eu acho que todas as três aqui vão ser sentimentos que vão ser gerados em cima de colaboradores, de acordo com a sua percepção. [...]

Na sequência, está disponível o Quadro 19, referente ao resumo de todas as categorias identificadas na análise dessa variável, assim como outras evidências das categorias vistas, finalizando a interpretação das variáveis constantes na dimensão Controles e Punições.

Quadro 19: Categorias da variável Monitoramento como Inibidor de Eventos de Segurança da Informação

Categorias	Frequência	Total de Evidências	Outras Evidências
Monitoramento consciente como orientador do comportamento	13	13	E2 - [...] Com certeza, o monitoramento faz as pessoas pensarem duas vezes antes de fazer. Eles sabem que alguém vai olhar, pode até não ser na mesma hora. Inibe as tentativas [...] E5 - [...] Se ele sabe que está sendo olhado, ele tende a se comportar bem melhor. [...] E8 - [...] Quando eles tem essa sensação de que estão sendo monitorados, consequentemente, diminui o nível de incidentes. Eles conseguem se controlar. "Tem alguém de olho na gente". Ou: "Tem alguém de olho nas atividades que eu estou fazendo" [...] E12 - [...] A partir do momento que o colaborador sabe que está sendo monitorado, ele vai tomar cuidado. Um ladrão não vai assaltar ninguém na frente do policial. Então, sim. Influencia de forma positiva no comportamento [...]
Dependência da percepção dos funcionários na inibição causada pelo monitoramento	2	3	E1 - [...] Eu acho que pode inibir. É que isso aqui depende muito do próprio funcionário, de como ele enxerga aquilo. [...] E3 - [...] Tem pessoas que não ligam ser monitoradas, não estão nem aí, e têm outras que tem uma preocupação enorme. [...]
Má intenção dos funcionários definindo o comportamento	1	1	E1 - [...] Quem quer agir de má fé, vai agir de má fé, não importa se tu estás coibindo, inibindo, etc. O problema não é a forma, ele vai tentar. Claro que ele vai ter uma dificuldade maior de fazer algo. [...]

Fonte: Elaborado pelo autor

A partir da conclusão da análise individual de todas as variáveis pertencentes ao Contexto de Tecnologia e Segurança da Informação, apresentaremos uma visão geral dessa dimensão segundo as influências percebidas das variáveis, mostradas no Quadro 20.

Quadro 20: Influências do Contexto de Tecnologia e Segurança da Informação no Comportamento Responsável

DIMENSÕES		VARIÁVEIS	INFLUÊNCIA PERCEBIDA
Contexto de Tecnologia e Segurança da Informação	Entendimento sobre TI e Segurança da Informação	Conhecimento e Habilidades	Não*
		Experiência e Conhecimentos Gerais em TI	Sim
		Conhecimento da Política de Segurança da Informação	Sim
		Severidade da Política de Segurança da Informação	Sim
	Controles e Punições	Mecanismos de Controle como Inibidores do Desempenho e da Criatividade	Inconclusiva
		Mecanismos de Controle da Violação de Regras e Normas	Não
		Punição como Inibidor da Reincidência de Eventos de Segurança da Informação	Sim
		Monitoramento	Sim
		Monitoramento como Inibidor de Eventos de Segurança da Informação	Sim

* Poucos indícios de influência não percebida

Fonte: O autor (2014)

De acordo com os resultados da análise interpretativa da influência do Contexto de Tecnologia e Segurança da Informação, é possível perceber que a maioria das relações de influência propostas em cada variável foram consideradas verdadeiras pelos gestores entrevistados, com exceção das variáveis Conhecimento e Habilidades, que faz parte do Entendimento sobre TI e Segurança da Informação, e Mecanismos de Controle da Violação de Regras e Normas, que é integrante da divisão Controles e Punições. É importante ressaltar que em uma variável pertencente à divisão Controles e Punições, a variável Mecanismos de Controle como Inibidores do Desempenho e da Criatividade, não foi possível definir se existe ou não uma relação de influência no comportamento responsável, pois não houve consenso

entre os respondentes, o que indica a necessidade da realização de outras pesquisas complementares para comprovar este fato. Em relação à intensidade de indícios encontrados nas variáveis, a única variável da dimensão Contexto de Tecnologia e Segurança da Informação que obteve poucos indicativos da relação de influência (nesse caso, a influência não percebida) foi Conhecimento e Habilidades, já que a diferença entre as respostas negativas e positivas dos gestores entrevistados foi mínima, o que sugere um estudo mais aprofundado futuramente neste item.

A seguir, a abordagem do Contexto Organizacional e suas influências no Comportamento Responsável dos colaboradores relacionado à Segurança da Informação será o tema da análise de conteúdo.

4.3 CONTEXTO ORGANIZACIONAL E COMPORTAMENTO RESPONSÁVEL RELATIVO À SEGURANÇA DA INFORMAÇÃO

Esta etapa do trabalho verifica a presença ou não da relação de influência percebida do Contexto Organizacional no Comportamento Responsável dos funcionários em relação à Segurança da Informação, a partir da análise de conteúdo categorial de cada variável que consta na dimensão avaliada, sendo que a interpretação será na mesma ordem definida no roteiro de entrevistas (ver Apêndice A), com uma questão para cada variável, o que atende o segundo objetivo específico.

A décima pergunta aborda a variável **Clima Organizacional**, componente da dimensão **Contexto Organizacional**, que está relacionada à percepção coletiva dos colaboradores em relação à organização. Primeiramente, observou-se a existência ou não de relação de influência do clima organizacional no comportamento responsável dos colaboradores, conforme a percepção dos respondentes, o que nos levou ao resultado unânime de 14 **respostas positivas**, confirmando a influência dessa variável no comportamento.

Na análise de conteúdo categorial dessa variável, a categoria que mais obteve frequência de citações foi **Evidências de relação direta entre clima organizacional e comportamento**, com seis observações e sete evidências descobertas. Essa categoria diz respeito a comprovações de fortes indícios da relação de influência entre clima organizacional e o comportamento adequado dos colaboradores, fator justificado pela fala do Gestor K:

> [...] As pessoas tendem a vestir mais a camisa da organização quando eles estão satisfeitos. Tem a política de Segurança e você sabe que tem uma maneira de burlar. Quando a pessoa veste a camisa, quando ela está bem na organização, quando o clima está favorável, ela tende a não fazer isso. Ela tende a não ir contra. [...]

O Gestor N também contribui para essa afirmação, conforme seu direto relato:

> [...] O clima organizacional está diretamente relacionado com o comportamento do colaborador que, por conseguinte, afeta a Segurança das Informações. Um clima favorável, um ambiente acolhedor e compromissado também instiga o comportamento responsável das pessoas em todos os sentidos, e com relação à Segurança da Informação não poderia ser diferente. [...]

Logo abaixo, no Quadro 21, são apresentadas todas as categorias observadas nesta variável, assim como outras informações relevantes para a caracterização das categorias.

Quadro 21: Categorias da variável Clima Organizacional

Categorias	Frequência	Total de Evidências	Outras Evidências
Evidências de relação direta entre clima organizacional e comportamento	6	7	E4 - [...] Se o clima organizacional não está legal, a tendência é que ela não siga critérios de Segurança de uma forma geral. [...] E6 - [...] uma vez que eu estou satisfeito na empresa, uma vez que o clima favorece, eu não vou fazer nada que eu sei que pode me colocar em risco. [...]
Comparação da influência do clima com a influência do ambiente de trabalho	2	2	E1 - [...] O clima influencia tanto quanto o ambiente organizacional [...] E2 - [...] O ambiente de trabalho como um todo influencia no comportamento. E com o clima organizacional não poderia ser diferente. [...]
Existência de pouca relação entre clima organizacional e comportamento	1	1	E1 - [...] O clima organizacional influencia, mas não sei se a influência é tão grande. Não vejo o clima organizacional tão relacionado com isso ainda. Acho que tem mais relação com os controles que existem. O clima organizacional, pontualmente, talvez vá influenciar algum grupo de pessoas que vão querer explorar alguma vulnerabilidade ou querer, conscientemente, praticar algum ato de desrespeito. Mas não sei se existe uma relação direta. Não tenho certeza. [...]
Pouca importância dos funcionários com o clima organizacional	1	1	E1 - [...] Sim. Isso, com certeza, influencia no comportamento. Mas aqui dentro, nós vemos que eles não se preocupam muito com isso. Não modifica o dia a dia deles. [...]

Fonte: O autor (2014)

Seguindo para a análise da questão 11, relativa à variável **Fluxo de Trabalho de Segurança da Informação**, também pertencente à dimensão **Contexto Organizacional**, podemos afirmar que ela se refere ao volume de práticas e procedimentos necessários para a manutenção da Segurança da Informação dentro de uma organização e sua influência no comportamento responsável dos empregados. No Quadro 22, encontra-se o resultado da análise da percepção dos gestores quanto a essa relação de influência.

Quadro 22: Influência da variável Fluxo de Trabalho de Segurança da Informação no Comportamento

Influência Percebida	Frequência
Sim	12
Não	2

Fonte: O autor (2014)

Como se pode notar, a relação de influência do fluxo de trabalho gerado pelos procedimentos necessários a serem realizados para garantir a Segurança da Informação no comportamento adequado dos colaboradores foi percebida por 12 entrevistados, com apenas duas respostas contrárias.

De acordo com a definição das categorias dessa variável, podemos classificar duas como as mais importantes pelo número de incidências: **Consciência da necessidade de práticas de Segurança** e **Preocupação com que regras de Segurança não interfiram nas atividades de negócio**. A categoria Consciência da necessidade de práticas de Segurança obteve cinco observações e evidências descobertas, retratando o conhecimento por parte de todos os envolvidos na Segurança da necessidade de procedimentos de Segurança da Informação para proteger os dados da organização contra ameaças. O Gestor L ilustra perfeitamente essa categoria:

> [...] Acontece, é normal isso. Não é só num processo corporativo, mas Segurança engessa processo na nossa vida também. Então, para determinado tipo de liberação de transação financeira, eu preciso estabelecer controles que, consequentemente, engessam. Aquela pessoa que libera um crédito de 1 milhão de reais para um cliente da instituição, não pode ser ela a única a fazer isso. Então, tem que ter um controle de alçada, de limites, que são intimamente ligados à Segurança, são controles de Segurança da transação. Então, não é porque eu sou um caixa de uma agência, que eu mesmo vou pegar e liberar um crédito no valor de 1 milhão. Não, não é bem assim. Tem que ter uma análise de crédito, tem que ter uma avaliação do cliente, tem que ter toda uma série de controles que acabam, não engessando, mas burocratizando mais o processo. Mas isso não é só quando nós falamos em corporação, isso é na nossa vida também. E é totalmente necessário. É mais do que válido, é necessário. [...]

Expondo a ansiedade dos gestores e da empresa em fazer com as regras e normas de Segurança da Informação não intervenham nos processos de negócio e nas atividades de todos os envolvidos, a categoria Preocupação com que regras de Segurança não interfiram nas atividades de negócio teve o mesmo número de citações e evidências da categoria anterior (cinco observações). Como forma de justificar a definição da categoria, o Gestor G define bem essa opinião:

> [...] Só que o que acontece é o seguinte: nós buscamos com que a Segurança, como eu já disse antes, não influencie nos negócios da empresa, que seja algo que permeie dentro da estrutura. Então, o fluxo de trabalho tem que ser conduzido de forma

> muito natural. Eventualmente, alguma ação possa trazer algum tipo de complicação inicial, mas, no dia a dia, a Segurança deve ser inserida no contexto de cada um, no desenvolvimento do sistema, na prática de trabalho, de qualquer coisa. Não pode ser um negócio que tranque o processo da empresa, jamais. [...]

Já o Gestor K ressalta a importância da conexão entre os processos e a Segurança da Informação:

> [...] Mas não se pretende que nenhuma parte da política de Segurança interfira no fluxo de trabalho. Normalmente, quando ocorre isso. “Não, agora está muito difícil de trabalhar dessa maneira”. Em sistemas de informação, por exemplo, nós tentamos ir lá, conversar, melhorar e até descobrir uma outra maneira de fazer. Tentar fazer com que a política, que as práticas de Segurança trabalhem junto com os processos, nunca barrem eles. [...]

Um resumo das categorias dessa variável pode ser observado no Quadro 23 disposto a seguir.

Quadro 23: Categorias da variável Fluxo de Trabalho de Segurança da Informação

Categorias	Frequência	Total de Evidências	Outras Evidências
Consciência da necessidade de práticas de Segurança	5	5	E1 - [...] As práticas de Segurança podem burocratizar as tarefas, mas são necessárias para evitar riscos. [...] E2 - [...] A ideia não é essa, mas os bloqueios são necessários para o andamento das atividades. [...]
Preocupação com que regras de Segurança não interfiram nas atividades de negócio	5	5	E2 - [...] nós tentamos, de qualquer forma, fazer a entrega final para ele. O que ele precisa na ponta, ele vai ter. É claro que nós tentamos fazer da melhor forma, da forma mais segura. [...] E5 - [...] Caso o fluxo de trabalho esteja muito comprometido e esteja trancando os processos de negócio da empresa, a política deve estar errada ou ultrapassada e deve ser revista e atualizada. [...]
Equilíbrio entre a quantidade de regras e o dinamismo da empresa conforme avaliação de risco	2	2	E1 - [...] deve ter um equilíbrio entre a quantidade de regras e também a necessidade da empresa ser dinâmica. E quem define este equilíbrio é o risco, a avaliação do risco. [...] E2 - [...] Toda e qualquer prática ou procedimento de Segurança da Informação está atrelada ao risco que tal atividade ou processo envolve. [...]
Praticas e procedimentos de Segurança como norteadores do comportamento adequado	1	2	E2 - [...] Eu tendo a dizer que, quanto mais procedimentos se tiverem, é melhor para a Segurança, porque os processos vão estar mais definidos e vai se garantir que eles vão ser seguidos da forma como eles foram estabelecidos. Não ter procedimentos ou ter poucos procedimentos, para mim, é malvisto, é pior. Porque a pessoa, para aquilo que ela tem procedimento, ela consegue na boa, consegue tranquilo. Para aquilo que ela não tem, ela vai ter que decidir sozinha e, às vezes, nem sempre ela toma a decisão correta. [...]
Compartilhamento da responsabilidade do risco com o setor envolvido	1	1	E1 - [...] E se não tiver como, nós vamos justificar o risco e assumir o risco junto com o responsável da área. Nós vamos expor: "Se ele acessar tal coisa, isso pode ocorrer, eu gostaria que tu me formalizasse por e-mail, pelo chamado, de que você está ciente de que isso pode acontecer". É flexível, mas reparte ou divide o risco com a área responsável. [...]
Necessidade de seguir regulatórios de Segurança	1	1	E1 - [...] Você precisa ter um compliance com, como eu citei antes, o Sarbanes-Oxley. Então, não é opcional, você precisa ter aquilo. Então, muitas vezes, os níveis adicionais vão ser mais do que um problema, vão ser pré-requisitos para a empresa operar no segmento em que ela se propõe a operar. [...]

Fonte: O autor (2014)

Em relação à variável **Cultura Organizacional**, correspondente à décima segunda questão do roteiro de entrevistas, temos o conjunto ou sistema de valores, hábitos e crenças estabelecidos e divulgados pela organização por meio de normas, atitudes e expectativas compartilhadas pelos colaboradores. Começando com a avaliação da percepção de influência notada pelos entrevistados, foi possível verificar a **confirmação** da relação de influência da cultura da empresa no comportamento considerado seguro dos empregados, pois todos os gestores ratificaram essa situação.

Entre as categorias mais citadas da variável Cultura Organizacional, temos: **Evidências de forte relação entre cultura organizacional e comportamento**, **Maior influência no comportamento em culturas com valores bem definidos** e **Dificuldade para manter práticas de Segurança em culturas de empresas de origem familiar**. Com a frequência de sete observações e evidências relatadas, a categoria Evidências de forte relação entre cultura organizacional e comportamento traz afirmações categóricas de uma relação íntima de influência entre os pressupostos básicos da organização e o comportamento responsável dos funcionários. O discurso do Gestor E pode representar essa categoria:

> [...] Se tem uma cultura, tu vai ter um ambiente organizacional. Influencia, no meu entendimento. Comunicação vai influenciar. Consciência das principais ameaças e familiaridade, isso tudo é influenciado pelo ambiente organizacional. Se você achar duas pontes diferentes no trabalho vai gerar um ambiente organizacional. Claro que a cultura vai influenciar isso diretamente. [...]

A categoria Maior influência no comportamento em culturas com valores bem definidos está relacionada com uma maior influência no comportamento responsável dos colaboradores em organizações que apresentam culturas fortes arraigadas. Com três observações e evidências relacionadas, a passagem relatada pelo Gestor F retrata bem o cenário dessa categoria:

> [...] As empresas que têm uma cultura forte têm uma influência maior. Se a empresa tem uma cultura de preservar processos, uma cultura com valores que são fortes, uma cultura onde isso é passado de uma forma bem incisiva para os funcionários, onde as pessoas vivem os valores da empresa, e os valores estão normalmente alinhados sempre com a política de Segurança, eu acho que isso tem uma influência grande. Porque aí a influência da pessoa observar regras, ela vem não só da política, mas ela vem do meio. Quando se vive isso na empresa, não só em relação à política de Segurança da Informação, mas em relação a outras políticas e outros valores da empresa. Não estou falando nem em políticas escritas no papel, mas uma pessoa que aprendeu a viver os valores da empresa, e ela tem incentivo, ela vê as pessoas praticando isso, ela vê os gestores praticando isso, ela vê colegas praticando isso, é claro que isso tem uma influência positiva na política de Segurança específica. [...]

Na categoria Dificuldade para manter práticas de Segurança em culturas de empresas de origem familiar, que também obteve três citações e evidências, é ressaltada a dificuldade em implantar e manter procedimentos e práticas de Segurança da Informação em organizações que apresentam culturas advindas de uma gestão familiar. A situação descrita pelo Gestor H justifica a categoria e evidencia os problemas apresentados nesse caso:

> [...] Aqui dentro, é um dos fatores que, às vezes, até nos atrapalha muito nessa parte da Segurança. Porque, como é uma empresa muito familiar, uma pessoa, um colaborador fica sabendo que outro colaborador tem um acesso maior ou significativo em relação ao dele e ele, prontamente, quer exatamente o mesmo acesso. Então, a própria cultura, um vai falando para o outro, o boca a boca, acaba influenciando, sim. Tem setores que, infelizmente, são influenciados pela grande

> cúpula. Presidente e diretores acabam dizendo: “nesse setor vocês não podem vetar tal coisa, não podem mexer tal coisa”. É bem cultural. Por ter pessoas da família, nós acabamos não conseguindo levar à risca a política de Segurança. [...]

Complementando o relato anterior, o Gestor I também verificou esses fatores:

> [...] Uma cultura de empresa familiar, por exemplo, o filho do dono sempre vai achar que ele pode acessar, o próprio dono. A figura do dono, não do executivo, já tem uma conotação diferente e, naturalmente, faz com que, por exemplo, uma política seja mais permissiva para o dono do que para os demais. Isso, naturalmente, já é um grande risco de Segurança, porque, como nós já comentamos antes, normalmente os executivos ou os donos ou as pessoas que têm cargos hierárquicos mais altos são as pessoas que, normalmente, têm mais informações da empresa, dos rumos e, naturalmente, também, podem, ou pelo menos, são os principais alvos de ataques ou de intenções maliciosas. [...]

O Quadro 24 mostra todas as categorias definidas na análise de conteúdo categorial, assim como a frequência, o total de evidências e outros relatos considerados interessantes.

Quadro 24: Categorias da variável Cultura Organizacional

Categorias	Frequência	Total de Evidências	Outras Evidências
Evidências de forte relação entre cultura organizacional e comportamento	7	7	E1 - [...] A cultura organizacional está diretamente ligada ao comportamento [...]
Maior influência no comportamento em culturas com valores bem definidos	3	3	E3 - [...] Uma empresa preocupada com Segurança, que tem valores e princípios baseados em Segurança, claro que vai influenciar positivamente no comportamento de seus colaboradores. [...]
Dificuldade para manter práticas de Segurança em culturas de empresas de origem familiar	3	3	E3 - [...] Em empresas familiares, é um pouco mais complicada a aceitação. Eu percebo que tem uma resistência maior. [...]
Necessidade de uma cultura voltada para a Segurança	1	2	E2 - [...] não adianta nada nós termos essa política bem estruturadinha se a cultura não demonstra que as pessoas devem ir nesse sentido. [...]
Pouca maturidade de Segurança por parte da cultura brasileira	1	1	E1 - [...] a maturidade do brasileiro para acesso, principalmente a acesso a internet em ambiente corporativo, ela é muito inicial, é uma maturidade quase infantil, em relação a maturidade de um funcionário na Europa. [...] Sabe, aí tem uma questão de infra-estrutura também. Na Europa, todo mundo tem acesso a internet, no Brasil, nem todo mundo. O cara usa a empresa para suprir essa necessidade de conexão que ele não tem em casa. [...] Sabe, é essa cultura que a gente tem. E isso não é só com TI, é com tudo, quando uma estrada é 100km/h a média, e não tem pardal, todo mundo vai a 120, 130km/h, porque não tem ninguém olhando mesmo. Na verdade, a política diz que não, mas se ele não é barrado, ou seja, se não tem um pardal, ele faz. Ele pensa assim, 'ah, é proibido, mas não tem ninguém olhando, não vai dar nada mesmo'. É a cultura do brasileiro que leva a isso. [...]
Similaridade de culturas em setores correlacionados	1	1	E1 - [...] É bem diferente esse tipo de mercado, tipo o Google e tudo mais, do que tu pegar indústria. Tu vai ver que todo mundo do ramo segue mais ou menos a mesma coisa. [...]
Pouca importância com Segurança por parte de culturas mais conservadoras	1	1	E1 - [...] Nós temos toda uma cultura dentro da empresa que, às vezes, prejudica a adoção de algumas práticas, nos limita na definição de algumas políticas, gerando vulnerabilidade e brechas na Segurança da Informação. A empresa é um pouco conservadora e isso afeta em algumas coisas, inclusive TI. A cultura da empresa também não exige muito um conhecimento e familiaridade com a política de Segurança por parte dos colaboradores, o que influencia no comportamento em geral. [...]
Comparação da influência da cultura com a influência do clima	1	1	E1 - [...] Assim como o clima, a cultura organizacional da empresa sempre vai influenciar no comportamento das pessoas. [...]

Fonte: O autor (2014)

Quanto à variável **Relação entre funcionários e seus superiores**, designada pela questão 13, que aborda o que pode afetar do relacionamento entre os colaboradores e seus

superiores no comportamento responsável relativo à Segurança da Informação, temos a seguinte relação de influência demonstrada no Quadro 25:

Quadro 25: Influência da variável Relação entre Funcionários e seus Superiores no Comportamento

Influência Percebida	Frequência
Sim	13
Não	1

Fonte: O autor (2014)

De acordo com a percepção de 13 gestores, o relacionamento dos empregados com os superiores **influencia** o comportamento responsável relativo à Segurança da Informação, fato que não foi confirmado apenas por um único entrevistado.

Entre as categorias que foram melhores avaliadas conforme a frequência de citações nessa variável, temos: **Bom relacionamento entre funcionários e superiores como facilitador do comportamento responsável** e **Evidências de influência positiva e negativa no comportamento**. Avaliando a boa relação entre colaboradores e superiores como um fator importante do comportamento considerado adequado na Segurança da Informação, a categoria Bom relacionamento entre funcionários e superiores como facilitador do comportamento responsável observou cinco citações e evidências relatadas. A partir da visão do Gestor I, pode-se ter uma noção da relevância dessa variável:

> [...] Sendo 70%, em média, dos problemas, internos, um bom relacionamento ajuda a minimizar sim, quando relacionado à má-fé, porque você acaba tornando aquele teu funcionário um cara aliado, preocupado com o negócio e, normalmente, isso inibe ou, pelo menos, reduz a probabilidade que ele tenha uma intenção nociva. Mas só isso não resolve. É bom ter esse comportamento, mas você basear ou, pelo menos, achar que isso é suficiente para resolver os problemas de Segurança, está longe disso. É bom, é uma boa prática. [...]

Conforme o relato do Gestor H, que traz uma situação específica onde somente o gerente da área recebe treinamento sobre Segurança e é ele quem deve repassar essa informação aos funcionários da área, essa relação de influência fica mais evidenciada:

> [...] nós fazemos algumas palestras, algumas coisas para conscientizar a Segurança aqui dentro e é passado só para o gestor da área. Se esse gestor tem a equipe na mão, e no caso, tem, a maioria dos setores tem, são exceções que não tem, eles conseguem trazer a equipe para o lado dele e passar a mensagem de uma forma correta, de uma forma eficaz para o nosso lado da Segurança. [...]

Na categoria Evidências de influência positiva e negativa no comportamento, relativa à presença de evidências de que a relação entre empregados e superiores pode causar tanto efeitos positivos quanto negativos no comportamento responsável, obteve três citações e

evidências descobertas. A síntese do Gestor E resume a categoria: “[...] O relacionamento entre chefes e subordinados sempre influencia, seja positiva ou negativamente no comportamento [...]”.

No Quadro 26, localizado abaixo, podemos verificar as categorias determinadas na análise da variável em questão e outras informações complementares.

Quadro 26: Categorias da variável Relação entre funcionários e seus superiores

Categorias	Frequência	Total de Evidências	Outras Evidências
Bom relacionamento entre funcionários e superiores como facilitador do comportamento responsável	5	5	E4 - [...] Quanto mais saudável for o relacionamento entre essas pessoas, melhor vai ser a aderência com relação à Segurança da Informação. [...] E5 - [...] O respeito ou a admiração dos colaboradores em relação aos chefes pode facilitar ou contribuir para o cumprimento da política e, consequentemente, para o comportamento adequado. [...]
Evidências de influência positiva e negativa no comportamento	3	3	E1 - [...] Pode, tanto para o bem quanto para o mal. [...]
Mau relacionamento entre funcionários e superiores como desencadeador de comportamentos inadequados	2	2	E1 - [...] O funcionário que não está satisfeito com a sua gerência, com a sua coordenação direta, ele tende a, é quase igual ao clima organizacional, tentar burlar alguma coisa, se ele quiser. Tende a vestir menos a camiseta da organização e ir contra porque ele não está satisfeito, provavelmente. [...] E2 - [...] Muitas vezes, um mau relacionamento entre funcionários e superiores pode fazer com que os colaboradores queiram tomar algum tipo de ação contra os seus superiores, de levar a informação da empresa porque ele quer sair da empresa e quer ficar com a informação para quando ele for para outra e ele não gosta mais da empresa por causa do chefe, algum tipo de sabotagem, algum tipo de situação que vá em detrimento ao superior imediato. [...]

Fonte: O autor (2014)

A próxima variável trata das condições de trabalho oferecidas pela organização, tais como situações de estresse, pressões, grande volume de trabalho, entre outras, a que os colaboradores estão sujeitos e que podem afetar no comportamento responsável relativo à Segurança da Informação destes, denominada de **Condições de Trabalho**, relacionada à questão 14. Para demonstrar a relação de influência percebida pelos entrevistados nesta variável, foi desenvolvido o Quadro 27.

Quadro 27: Influência da variável Condições de Trabalho no Comportamento

Influência Percebida	Frequência
Sim	12
Não	2

Fonte: O autor (2014)

Nota-se que a influência das condições de trabalho oferecidas pela empresa no comportamento adequado dos funcionários relacionado à Segurança da Informação foi **confirmada** por 12 gestores, com somente dois casos contrários verificados.

De acordo com as categorias descobertas na interpretação das entrevistas, podemos destacar a categoria Condições de trabalho desfavoráveis como facilitador do comportamento inadequado, com frequência de nove citações e mesmo número de evidências. O parágrafo relatado pelo Gestor I exemplifica situações corriqueiras que podem afetar o comportamento:

> [...] A questão do volume de trabalho, quanto maior o volume de trabalho, maior a probabilidade de erro, de você passar um e-mail, como acontece muito, você coloca um e-mail com meu nome, que é super comum, aí você coloca o nome e vai ter 500 no Outlook que ele vai tentar auto-completar ali, e se você, de repente, tem duas pessoas com o sobrenome parecido, daqui um pouco, você manda um e-mail para outra pessoa. Então, o volume de trabalho, o estresse, a posição. Então, de repente, um executivo que é muito cobrado ou que tem que gerar muitos relatórios ainda manuais porque não tem sistemas que preveem isso, não ter sistemas adequados, ter que fazer muitos trabalhos manuais, deixar planilhas espalhadas por vários locais, você dar muitos equipamentos de mobilidade e não ter política adequada nem ferramentas de controle. [...]

O Gestor J também relata casos onde condições de trabalho irregulares contribuíam para o comportamento errôneo dos envolvidos:

> [...] Estresse, temperatura da sala, luminosidade, qualquer coisa desse tipo, eu acho que também está relacionada. Salas muito apertadas, eu já vi situações como essa. Pegar clientes que os caras não tinham espaço nem para se mexer dentro das empresas. Então, Segurança era a última coisa que eles estavam preocupados. Eles estavam mais preocupados com o bem-estar deles, com os caras conseguirem trabalhar de uma forma mais humana, assim vamos dizer. Ou então, um lugar que tinha, que eu já fui, que o ar condicionado estava quebrado ou a sala não funcionava direito porque o ambiente de trabalho era ruim, não era adequado, e as pessoas acabavam se sentindo mais desmotivadas por causa disso. E claro, influencia negativamente em relação à Segurança. [...]

Abaixo, no Quadro 28, são mostradas todas as categorias desenvolvidas na análise dos dados das entrevistas relativas à variável Condições de Trabalho.

Quadro 28: Categorias da variável Condições de Trabalho

Categorias	Frequência	Total de Evidências	Outras Evidências
Condições de trabalho desfavoráveis como facilitador do comportamento inadequado	9	9	E5 - [...] O estresse e a entrega de metas forçam com que eles procurem um atalho, uma forma de fazer as coisas não daquela forma que está escrita na política. Então eles tentam fazer aquela entrega rápida de forma a burlar o sistema ou de forma que não é indicada. Isso, com certeza, influencia. [...] E9 - [...] se ela está sofrendo um nível de pressão muito grande por resultado, se ela está trabalhando num ambiente com alto nível de estresse, ela pode estar se armando, se preparando para sair da empresa a qualquer momento e isso está promovendo ela a levar informação, vazar informação, tentar algum evento fraudulento contra a organização, porque ela não concorda com a forma como a empresa está atuando com ela. [...]
Práticas de Segurança acima das condições de trabalho	1	1	E1 - [...] Tem que se adequar. Ele pode estar estressado por outras coisas, mas ele tem que se adequar às normas porque ele sabe que pode ter algum tipo de penalização depois. [...]

Fonte: O autor (2014)

Abordando a pergunta 15, que diz respeito aos diferentes ambientes organizacionais, tais como ambientes onde a cooperação é priorizada ou ambientes no qual a competição faz parte do cotidiano, e suas influências no comportamento adequado dos colaboradores frente à Segurança da Informação. A relação de influência percebida pelos entrevistados na variável chamada de **Diferenças entre Ambientes Organizacionais** pode ser vista no Quadro 29.

Quadro 29: Influência da variável Diferenças entre Ambientes Organizacionais no Comportamento

Influência Percebida	Frequência
Sim	12
Não	2

Fonte: O autor (2014)

Segundo 12 dos 14 gestores entrevistados, **existe** influência dos diferentes tipos de ambientes organizacionais no comportamento responsável dos empregados de forma diferenciada, fato que não foi confirmado por apenas dois respondentes.

Em relação às categorias desvendadas na interpretação dessa variável, a mais significativa foi **Dificuldade de aplicação da política de Segurança em ambientes competitivos**, com seis considerações e sete evidências. Trata-se da dificuldade encontrada pela gestão em aplicar e fazer com a Política de Segurança seja cumprida pelos colaboradores em ambientes onde o nível de competição é mais elevado, o que foi relatado no caso vivenciado pelo Gestor H na empresa onde ele trabalha:

> [...] Sim, isso pode influenciar na Segurança e isso ocorre aqui dentro. Tem setores que os responsáveis têm os colaboradores na mão, assim como tem setores que é uma luta para ele tentar pegar aquela posição de gestor da área e isso acaba em querer saber o quanto que o fulano recebe, quanto que é a folha de pagamento, se o cara está com a máquina aberta, não está bloqueada, ela vai dar uma olhada nos e-mails do cara tentando ver se ele não tem algum e-mail que possa fazer com que ele seja derrubado daquele setor. Então, existe isso. O cara deixou uma tela aberta, digamos do contracheque, foi no banheiro e voltou, outro vai lá olhar quanto o fulano está ganhando. É uma forma de pressionar para eu pegar o lugar dele. Isto ocorre e existe aqui dentro, sim. [...]

O exemplo ilustrado pelo Gestor I também relata um fato trivial que pode ocorrer e afetar a Segurança da Informação:

> [...] Isso é bem comum em equipe de vendas, comercial. Se nós falarmos de Segurança em bancos, nós sempre lembramos de Segurança em exemplos bancários, e hoje os gerentes de organizações são extremamente cobrados por metas, vendas de seguros, vendas de uma série de produtos financeiros. Então, sim. Isso até entre os funcionários e até, eventualmente, entre o funcionário e o cliente, porque, por exemplo, é possível que um gerente de banco passe uma informação para um cliente por e-mail para tentar acelerar um processo que ele teria que visitar porque ele tem que bater a meta. Isso eu já vi acontecer. Alguma informação que a política do banco não permite que seja passada por e-mail, ele mandar alguma orientação financeira ou algum extrato, resumo financeiro por e-mail, que ele não poderia, para que ele pudesse cumprir a meta porque era o último dia do mês e ele precisava bater. Então, sim. Isso é um exemplo claro de que isso afeta. [...]

A segunda categoria mais citada foi **Displicência de práticas de Segurança em ambientes cooperativos**, com quatro observações e evidências relatadas. Relacionada à falta de cuidado e de atenção que um ambiente onde a cooperatividade entre os membros é favorecida pode proporcionar, pode-se verificar na citação do Gestor I a justificativa dessa abordagem:

> [...] Em ambientes cooperativos também, daqui a pouco, todo mundo acha que, por que está no mesmo time, pode trocar as senhas ou pode trocar arquivos de mesmo projeto, ou começam, daqui um pouco, dois times de áreas diferentes começam a querer trocar informações dos seus projetos, e isso, naturalmente, pode ocasionar algum vazamento de informação, alguma displicência em relação à Segurança. [...]

Facilidade de entendimento e aplicação da política de Segurança em ambientes cooperativos foi a terceira categoria melhor qualificada nesta variável, com três observações e evidências justificadas. Ambientes cooperativos facilitam as relações entre as pessoas, o que pode proporcionar maior compreensão dos colaboradores e facilitar a adoção de práticas e procedimentos dispostos na Política de Segurança da Informação, conforme o que foi dito pelo Gestor F e que também pode ser considerado o contraponto da categoria anteriormente analisada:

> [...] Sempre que existe um ambiente cooperativo, claro que eu acho que vai ficar mais fácil você seguir, respeitar e, principalmente, entender e adotar a política. Mais do que seguir e do que respeitar, você entender para que serve, entender qual o valor dela e assumir aquilo realmente com uma regra pessoal do que só alguma coisa que está escrito. [...]

Disposto logo a seguir, o Quadro 30 observa todas as categorias expressas na análise de conteúdo dessa variável.

Quadro 30: Categorias da variável Diferenças entre Ambientes Organizacionais

Categorias	Frequência	Total de Evidências	Outras Evidências
Dificuldade de aplicação da política de Segurança em ambientes competitivos	6	7	E4 - [...] em ambientes competitivos, quando a própria equipe está dividida em busca de objetivos, isso eu considero que dá margem a buscar alternativas de competição e pode tornar a interpretação das regras de Segurança equivocada. [...] E6 - [...] num grupo mais competitivo, elas estão mais preocupadas com manter seus próprios empregos ou se diferenciar internamente pela empresa. Então, os caras vão procurar se destacar em relação a outros grupos ou outras pessoas e a Segurança ficaria em segundo plano. [...] E7 [...] a competitividade por si só trás certa ambiguidade ao ambiente, o que pode favorecer ou incitar uma pessoa a ter atitudes inadequadas no que diz respeito à Segurança da Informação [...]
Displicência de práticas de Segurança em ambientes cooperativos	4	4	E2 - [...] Num ambiente cooperativo, existem casos da pessoa usar o usuário de outra. Isso é um incidente de Segurança, mas não ocorrem vulnerabilidades diretas. Existe um conhecimento das duas partes. [...] E3 - [...] Num ambiente cooperativo, ele pode ter um maior nível de parceria entre os funcionários e a informação transitar de uma forma menos controlada. [...]
Facilidade de entendimento e aplicação da política de Segurança em ambientes cooperativos	3	3	E2 - [...] Se você tem um grupo mais coeso, a tendência é que as pessoas se sintam mais confortáveis em seguir normas de Segurança da Informação. [...] E3 - [...] Um ambiente cooperativo pode fazer com que as pessoas sejam mais conscientes em relação à Segurança por causa do trabalho em equipe [...]
Maior Segurança da Informação em ambientes excessivamente competitivos	2	3	E1 - [...] Um excesso de competitividade pode fazer com que as pessoas protejam mais as informações porque elas não querem que outros colegas tenham acesso a determinado tipo de dados para não terem privilégios em relação a resultados que elas tenham. [...] E3 - [...] No ambiente competitivo, como existe uma competição entre os próprios colaboradores, o cuidado com a Segurança da Informação pode ser maior, pelo fato de que ninguém quer expor nada para o outro. [...]
Necessidade dos funcionários estarem preparados diante de diferentes ambientes organizacionais	1	1	E1 - [...] Quem trabalha em ambientes diferentes já sabem o que vão enfrentar e devem estar preparados para isso. [...]
Negligência de práticas de Segurança em ambientes excessivamente cooperativos ou competitivos	1	1	E1 - [...] Ambientes muito cooperativos ou competitivos podem fazer com que a Segurança seja relaxada no dia a dia de funcionários ou, eventualmente, você tem aí uma incitação à má-fé. [...]
Necessidade de conscientização da Segurança em todos os ambientes	1	1	E1 - [...] é importante que, mesmo tendo a competição, e sempre há competição, mesmo em ambientes cooperativos existe um nível de competição, sempre tem que ter, antes de mais nada, uma conscientização de que o nível de Segurança é necessário e adequar a isso. [...]

Fonte: O autor (2014)

Como sendo a próxima variável a ser analisada, temos o **Comportamento dos Pares**, relacionada com a pergunta 16 do roteiro de entrevistas, que trata da influência dos colegas de trabalho mais próximos no comportamento responsável dos colaboradores relativo à Segurança da Informação. A partir da percepção de todos os 14 gestores entrevistados, foi **confirmada** a existência da relação de influência dos colegas de serviço no comportamento adequado dos funcionários.

Entre as categorias mais citadas desta variável, está a categoria **Tendência em seguir o comportamento dos colegas de trabalho**, que aborda à disposição em acompanhar o comportamento dos pares (colegas de serviço mais próximos), tanto em comportamentos considerados adequados quanto inadequados. Com seis observações e evidências dispostas, a fala do Gestor J caracteriza a situação descrita pela categoria:

> [...] Muitas vezes, a pessoa enxergando que o outro colega segue as normas de Segurança ou adota um comportamento seguro, ela se sente constrangida de não seguir. Vou dar um exemplo. Aqui nós temos uma política e já está arraigada na nossa cultura. Sair da frente da máquina, eu bloqueio a estação. Aqui, dificilmente, alguém não faz isso. E quem não faz, acaba sendo motivo de piada ou nós tiramos onda, alguma coisa nesse sentido. Então, o pessoal sempre segue. E quando não segue, às vezes, o pessoal acaba entrando, mudando o fundo de tela, mandando um e-mail para ele mesmo, fazendo alguma brincadeira assim, saudável, no sentido de dizer: 'te liga que você não está seguindo a política'. Então, acaba o pessoal influenciando nesse sentido, um acaba influenciando o outro nesse sentido. [...]

A síntese do Gestor D pondera real e fielmente a categoria encontrada: "[...] Então, na verdade, o funcionário funciona, na minha visão, 'Maria vai com as outras'. Se tem uma bagunça, o cara vai viver na bagunça. Se ele vê tudo organizado e tem regras, o cara segue as regras, tirando exceções, é claro [...]".

A outra categoria mais significativa foi **Tendência em manter o comportamento de acordo com o ambiente de quando entrou na empresa**, com três citações e mesmo número de evidências localizadas. Essa categoria aborda a intenção de continuar com o mesmo comportamento que o colaborador sempre teve desde que iniciou seu trabalho em determinada organização, situação disposta no relato do Gestor I:

> [...] Então assim, o comportamento em geral, esse comportamento de massa assim, você vai ter um comportamento, normalmente, aderente. Tem até aquela experiência dos macaquinhos com bananas, aquela coisa toda. Então, sim. Influencia. Você tem um ambiente com que todas as pessoas estão preocupadas em manter as suas senhas, que não divulgam suas senhas, naturalmente, você vai aderir àquele modelo de trabalho. Em compensação, se você chega num lugar, todo mundo sabe a senha de todo mundo, você chega, como eu canso de ver em agências bancárias, hoje cada vez menos, porque eu não vou muito à agência, mas você vê assim: "Fulano, loga aqui para mim porque eu preciso fazer assim". Duas coisas. Primeiro: se o cara está pedindo para alguém logar para ele, quer dizer, ele não tem acesso. Se ele não tem

> acesso, ele não pode estar logado com senha de ninguém. E a outra coisa é: o cara está passando o login que é dele e o cara está fazendo uma operação no sistema. Então assim, são coisas que, na verdade, o comportamento coletivo vai determinar. Se você acha aquilo normal, mais um chegar e pedir: “loga aqui para mim”. É você entrar na empresa e amanhã você está pedindo, se aquilo é um comportamento normal. [...]

O caso acontecido na organização onde o Gestor D trabalha e que foi relatado na entrevista afere a veracidade e a importância da categoria descrita:

> [...] O comportamento, na minha visão, o comportamento do funcionário com relação à Segurança da Informação depende do cenário que ele enxerga quando ele entra na empresa. Então tu vai pegar pessoas que, por exemplo, nós implementamos uma política de Segurança da Informação mais rígida a partir de 2007, início de 2008. Foi possível ver pessoas que entraram antes disso, quando tínhamos um ambiente mais brando quanto a isso, elas continuavam tendo a visão do passado e não aceitando a política, e quem já entra no novo ambiente não há isso, já entra mais atento. Se você constrói um ambiente organizacional e condições de trabalho visando isso, ou seja, ele já entra sabendo que são essas as regras, que é assim que funciona, se ele vê todo mundo agindo daquela maneira, a pessoa nova quer ser aceita, então ela vai seguir. Agora se ela entra em uma empresa em que, uma, ou você não tem um ambiente organizacional solido, condições de trabalho adequadas e vê todo mundo fazendo o que quer, naturalmente, ela vai seguir a fazer o que quer, porque ela não vai querer ser o “Caxias”. [...]

Para resumir todas as categorias descobertas na interpretação dos dados dessa variável, veja o Quadro 31, disponível a seguir.

Quadro 31: Categorias da variável Comportamento dos Pares

Categorias	Frequência	Total de Evidências	Outras Evidências
Tendência em seguir o comportamento dos colegas de trabalho	6	6	E4 - [...] É um efeito cascata. As pessoas tendem a seguir o comportamento dos colegas mais próximos. [...] E6 - [...] Uma pessoa, vendo os colegas de trabalho tendo ações responsáveis no que diz respeito à Segurança da Informação, tende a seguir essas mesmas ações. No entanto, isso também vale para o caso negativo. [...]
Tendência em manter o comportamento de acordo com o ambiente de quando entrou na empresa	3	3	E3 - [...] Se todos no ambiente de trabalho não têm comportamentos responsáveis, a pessoa que tiver observando ou recém chegada na empresa também não vai ter. [...]
Variação do comportamento de seguir os colegas conforme cada indivíduo	2	2	E1 - [...] Nós temos a situação da pessoa que deixa a senha escrita em cima do teclado. Tanto é, de uma pessoa do lado pensar que realmente é certo e fazer o mesmo, como é de uma pessoa do lado dizer que você está fazendo errado, que você não pode fazer isso, e a pessoa parar de ter essa prática. [...] E2 - [...] O colaborador que vê um colega tendo um acesso indevido pode ter duas ações, ele não concordar com aquilo ou ele pode concordar com aquilo. E se ele concordar com aquilo e achar que vai ser bacana para ele fazer também, ele vai ter o mesmo tipo de atitude que a pessoa que está tendo um comportamento irresponsável. É algo muito comportamental. Então, a pessoa pode ser mais fácil ou menos facilmente influenciada. Então, o comportamento, efetivamente, influencia. Como a engenharia social. [...]
Necessidade de não imposição do comportamento em relação à Segurança	1	1	E1 - [...] no momento que tu constrói um ambiente organizacional e um ambiente de trabalho que permitam uma validação da Segurança da Informação, que as pessoas tenham noções daquilo, essa questão do comportamento em relação à Segurança da Informação se torna um negocio que não pode ser imposto. Se tu impuseres, a pessoa não vai. Obrigada, ela não vai fazer. Ela tem que ver que todo mundo faz, e ela naturalmente vai fazer também. [...]

Fonte: O autor (2014)

Na última variável da dimensão Contexto Organizacional, **Satisfação com o Trabalho**, relacionada com a pergunta 17 do instrumento utilizado na pesquisa, que aborda a satisfação individual do colaborador com o seu trabalho e sua influência no comportamento responsável frente à Segurança da Informação, **foi percebida** a relação de influência da variável no comportamento por todos os 14 gestores entrevistados.

A categoria melhor classificada em relação à frequência de citações foi **Influência da insatisfação do funcionário no comportamento inadequado**, com oito observações e evidências notificadas. O exemplo prático contado pelo Gestor H, vivenciado por ele na empresa onde trabalha, relata perfeitamente a influência da insatisfação no comportamento:

> [...] Se ele não está muito satisfeito, aqui já ocorreram dois incidentes a respeito disso. Vou contar um caso prático. Tinha um evento, que é uma semana da CIPA,

> tem palestras sobre diversos assuntos, tabagismo, isso e aquilo, e um funcionário que não estava muito satisfeito com o trabalho pegou e aproveitou-se de um momento que um computador estava aberto com outra identidade que não era a dele e mandou um e-mail global, para todos, dizendo que essa semana era tal coisa, que ele queria era dinheiro, que não queria participar disso, que ele estava perdendo tempo. Acabou dando rumores lá na diretoria, na parte da presidência, e que isso não poderia acontecer. Então, pode influenciar. O cara insatisfeito vai procurar mostrar que ele não está satisfeito, às vezes de uma forma correta, às vezes também de uma forma equivocada, de má fé. Isso influencia. [...]

Em seu comentário, o Gestor F frisa que o funcionário que não está plenamente satisfeito com seu emprego se sente fora dos padrões e valores estabelecidos pela organização, o que favorece o comportamento inadequado:

> [...] O funcionário insatisfeito, aquele que não está bem no meio dele, naturalmente já está mais desligado dos valores da empresa, ou seja, não está vivendo os valores da empresa, já está desconectado da empresa, então, certamente ele está mais propenso a não entender os valores, ir contra os valores da empresa, e, por consequência, ir contra também às regras que existem dentro da empresa. Isso é natural. [...]

Já para o Gestor L, um colaborador insatisfeito pode se apoderar de alguma informação da organização para usufruo próprio, conforme sua citação:

> [...] O funcionário insatisfeito pode ser motivado a ter alguma ação contrária no que diz respeito à Segurança da Informação para ter algum benefício próprio como algum benefício financeiro ou alguma informação que ele quer levar da empresa para as suas próximas oportunidades de trabalho, para projetos particulares, o que quer que seja. [...]

Todas as categorias selecionadas podem ser vistas no resumo disposto no Quadro 32 para apreciação.

Quadro 32: Categorias da variável Satisfação com o Trabalho

Categorias	Frequência	Total de Evidências	Outras Evidências
Influência da insatisfação do funcionário no comportamento inadequado	8	8	E5 - [...] Se a pessoa não está satisfeita com o trabalho, ela tende a não dar tanta importância para a Segurança da Informação. Inclusive, já presenciei situações onde o funcionário estava insatisfeito com a sua gestão e acabou fazendo esse tipo de coisa. [...] E6 - [...] Um funcionário insatisfeito, às vezes, quer ser demitido e vai acabar tentando fazer ou burlar o sistema. Um funcionário insatisfeito tem mais chances de tentar burlar ou ignorar a política de Segurança. [...] E8 - [...] Pode ser que um funcionário insatisfeito tenha comportamentos indevidos em relação à Segurança por causa de uma indisposição com algum chefe, por exemplo, por causa de alguma particularidade que aconteceu com ele e que ele julgue injusta. [...]
Influência da satisfação do funcionário no comportamento responsável	2	2	E1 - [...] Pode influenciar de uma maneira favorável. Talvez não negativa, porque sempre o lado negativo, ele bate nas regras e nas normas. De maneira positiva, ele influencia e gera um bem estar na aplicação do ambiente de forma segura. [...] E2 - [...] o funcionário satisfeito, eu acho que ele vai estar mais disposto a apontar algum problema. "Eu entrei no site tal, que é um site do meu trabalho, eu preciso desse site para trabalhar". Ou: "o e-mail que eu recebi do fornecedor foi bloqueado pelo filtro de e-mail", para que a política auxilie o processo de trabalho dele. Ele vai estar mais preocupado com trazer Segurança ao processo dele. [...]
Influência positiva e negativa da satisfação no comportamento	2	2	E1 - [...] Acho que a satisfação individual pode influenciar positiva e negativamente no comportamento [...]
Preocupação com a satisfação do funcionário	1	1	E1 - [...] o que me preocupa mais não é a criatividade e sim a felicidade do usuário. [...] os funcionários não gostam, os novos funcionários, principalmente, não gostam do computador que a gente dá para eles porque em casa eles têm um bem melhor, eles não gostam do telefone que a gente dá para eles porque o telefone celular não tem o que eles gostam que tenha, não é um smartphone. Então, a gente está começando a ver como a gente vai lidar com isso [...] Está relacionado com o bem estar, ele estar satisfeito com os recursos e da maneira como ele trabalha, com os recursos disponibilizados a ele. Daqui a pouco ele vai ir para outra empresa, recebendo o mesmo salário e que ele tem os brinquedinhos ou os recursos que ele acha mais divertido durante o dia. Isso realmente é uma preocupação e a gente discute, o problema é como encontrar o meio termo. [...]
Permissividade da política de Segurança da Informação	1	1	E1 - [...] Se você perceber que precisa acessar algo, o Youtube. Por exemplo, o Youtube é bloqueado. Você fala com seu diretor que vai ter um ganho no trabalho e tal, se tiver o Youtube. Isso é trazido para nós e OK, porque é conteúdo. [...]
Atenção especial aos funcionários insatisfeitos quanto à Segurança da Informação	1	1	E1 - [...] Então, à pessoa insatisfeita, sempre tem que ser atribuído um nível de atenção diferenciado, porque ela tende, nós estamos falando de insatisfação com salário, com o chefe, com n situações, a ser mais propensa a gerar um incidente de Segurança da Informação. [...]

Fonte: O autor (2014)

Com o término da análise da última variável da dimensão Contexto Organizacional, seguimos para uma interpretação holística dessa dimensão e suas variáveis influenciadoras do comportamento, a partir do Quadro 33.

Quadro 33: Influências do Contexto Organizacional no Comportamento Responsável

DIMENSÕES	VARIÁVEIS	INFLUÊNCIA PERCEBIDA
Contexto Organizacional	Clima Organizacional	Sim
	Fluxo de Trabalho de Segurança da Informação	Sim
	Cultura Organizacional	Sim
	Relação entre Funcionários e seus Superiores	Sim
	Condições de Trabalho	Sim
	Diferenças entre Ambientes Organizacionais	Sim
	Comportamento dos Pares	Sim
	Satisfação com o Trabalho	Sim

Fonte: O autor (2014)

Segundo a interpretação das variáveis descritas, é possível confirmar a relação de influência percebida do Contexto Organizacional no Comportamento Responsável dos empregados Relativo à Segurança da Informação, visto que todas as variáveis pesquisadas desta dimensão foram consideradas influenciadoras do comportamento responsável pelos respondentes. Quanto à intensidade dos indícios encontrados nas variáveis relatadas, todas foram avaliadas como de forte relevância, uma vez que a diferença entre as respostas positivas e negativas foram de larga amplitude.

Na próxima fase de apresentação dos resultados, serão abordadas as influências percebidas do comportamento responsável frente à Segurança da Informação no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação.

4.4 COMPORTAMENTO RESPONSÁVEL RELATIVO À SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO CONTRA VULNERABILIDADES A AMEAÇAS INTERNAS DE SEGURANÇA DA INFORMAÇÃO

Esta etapa dos resultados da pesquisa examina a presença ou não da relação de influência percebida do Comportamento Responsável Relativo à Segurança da Informação dos colaboradores na Proteção Contra Vulnerabilidades a Ameaças Internas de Segurança da

Informação, o que contempla o terceiro objetivo específico. Toda a análise das variáveis seguiu a sequência das questões dispostas no roteiro de entrevistas adotado (ver Apêndice A), onde cada pergunta equivale a uma variável. É importante salientar que a dimensão Moderadores do Comportamento Responsável, que aborda os fatores moderadores do comportamento dos colaboradores, também será observada neste item.

A variável **Disseminação do Comportamento**, correspondente à décima oitava questão, retrata as diversas formas de disseminação do comportamento responsável utilizadas pelas organizações, principalmente o uso da Política de Segurança como elemento fundamental na difusão da conduta considerada adequada aos colaboradores a fim de evitar vulnerabilidades a ameaças internas de Segurança da Informação. Com relação às maneiras mais utilizadas pelas empresas na divulgação do comportamento entre os funcionários, o Quadro 34 traz todas as formas de comunicação citadas pelos respondentes e que são empregadas em suas respectivas organizações.

Quadro 34: Formas de Disseminação do Comportamento Responsável a fim de evitar Vulnerabilidades a Ameaças Internas

Formas de Disseminação do Comportamento Responsável	Frequência
Política de Segurança da Informação	12
Intranet	10
Informativos	6
Documento assinado quando entra na empresa	6
Treinamentos / Programas de conscientização	4
Softwares	2
Gestão da Política de Segurança da Informação	1

Fonte: O autor (2014)

Conforme o esperado, a Política de Segurança da Informação é o **principal** disseminador do comportamento responsável, com 12 afirmações. Somente dois entrevistados disseram não utilizar a Política de Segurança dessa maneira, fato justificado por não existir um documento específico sobre Segurança da Informação em suas respectivas organizações (ver Quadro 33). A intranet da empresa é outra forma de divulgação do comportamento bastante evidenciada, o que também é explicado por ser onde a Política de Segurança está disponível em tempo integral para acesso de todos os funcionários. Termos de compromisso

firmados quando da entrada do colaborador na organização e informativos como cartazes, murais, e-mails de comunicação e publicações internas também foram lembrados como difusores do comportamento. Apesar de serem considerados de extrema relevância para a conscientização dos funcionários por diversos autores referenciados, os treinamentos ou programas de conscientização foram mencionados por somente quatro gestores.

Quanto às categorias identificadas nesta variável, a mais significativa foi **Melhores formas de exposição do comportamento desejável**, com 10 observações e evidências encontradas. Relacionada com a descrição das maneiras mais efetivas de divulgação do comportamento responsável, esta categoria pode ser definida pelo relato do Gestor D:

> [...] Política da Informação Administrativa 002. Ela está dentro da intranet. Todo funcionário, quando entra, ele assina um documento que tem os principais pontos. A política de informação ao todo tem 32 páginas, mas ninguém na empresa vai ler ela toda. Lá a gente colocou os principais, tem questão de e-mail, questão de acesso, questão de internet e questão de senha. Lá também estão descritas as punições caso desobedeça. Tem sanções disciplinares que vão desde advertência formal até demissão por justa causa, dependendo do que está fazendo. E o funcionário assina e isso fica na pasta dele. Isso faz com que nenhum funcionário possa alegar que não sabia. Tu podes realmente aplicar as sanções disciplinares oficiais porque ele assinou. Se ele leu ou não leu, isso é problema dele. Então, tem essa política, que é revisada a cada seis meses. Mas é na política de Segurança da Informação. Na verdade, quando ele tenta enviar um e-mail, ele vai receber um aviso na tela. Tem a comunicação duas a três vezes por semestre de botar no mural, mandar e-mail informando as regras de utilização. É isso.

Já para o Gestor I, a melhor forma para expor o comportamento varia conforme a empresa ou o setor a ser aplicada a Política de Segurança:

> [...] É na política que tem que ser, mais do que construída no papel, ela tem que ser divulgada internamente, tem que ser exposta para o funcionário e o funcionário tem que dar o consentimento formal, tem que ler e aceitar os parâmetros dessa política. E toda e qualquer alteração deve ser atualizada para o funcionário e deve ser revalidado o entendimento do usuário. Mas é na política. Na nossa empresa, é na intranet. Eu, honestamente, acho que é o melhor lugar, mas tudo depende da empresa. Então, por exemplo, daqui a pouco você tem um chão de fábrica e o funcionário não vai ter acesso a uma intranet, mas aí você pode ter uma cartilha de Segurança com formato de gibi, de revistinha em quadrinhos, e você pode divulgar para os que têm acesso, eventualmente. Porque a brecha de Segurança não está, na verdade, só associada hoje ao computador associado ao funcionário. Se você tem um chão de fábrica num processo produtivo de um lançamento de um calçado e esse funcionário entra com celular, e o celular hoje tem câmera de 5 megapixels, você tem que informar para ele que ele não pode entrar com o celular. Então, isso vai ser feito diretamente no RH, na entrada dele, pode ser feito ciclos de treinamento. Aí cada empresa tem que encontrar o seu formato. Na nossa empresa, a intranet é mais do que adequada e nós utilizamos, até por ser ecologicamente melhor, não tem papel impresso, coisa e tal. [...]

No Quadro 35 estão localizadas todas as categorias descobertas na análise desta variável, bem como a frequência de observações e outras evidências importantes.

Quadro 35: Categorias da variável Disseminação do Comportamento

Categorias	Frequência	Total de Evidências	Outras Evidências
Melhores formas de exposição do comportamento desejável	10	10	E1 - [...] por exemplo, saiu um quiz no nosso jornal de circulação interna, o qual veio na capa e no centro do jornal. Tinha duas páginas. Eu gosto de fazer um quiz para falar os conceitos sobre a área de TI. No treinamento atual, nós temos questionário, no treinamento virtual tem um questionário. [...] E2 - [...] Na política, que está em várias formas. No treinamento, como eu já falei. Em vários momentos, painéis, nós temos murais, tem várias formas de divulgação da política. A empresa tenta sempre utilizar meios de comunicação. Está na intranet a política, tem treinamentos periódicos, divulgação, tem softwares que avisam porque está bloqueando alguma coisa. [...] E5 - [...] É sempre numa política de Segurança. Na verdade, em dois lugares, na política e nas campanhas ou nas palestras de conscientização. Então, caso a pessoa não leia a política [...]
Inexistência de um documento específico sobre a conduta em relação à Segurança da Informação	2	2	E1 - [...] Nós temos na nossa intranet uma página que fala sobre conduta do colaborador dentro da empresa. Ela é genérica no sentido de que ela não trata especificamente no que diz respeito à Segurança da Informação, é a conduta do colaborador dentro da empresa, mas ela contempla assuntos de Segurança da Informação, então a intranet seria o caminho. [...] E2 - [...] Nós temos os informativos na tela. Quando a pessoa não olha, nós enviamos e-mails periodicamente com orientações aleatoriamente [...]
Dificuldades de exposição do comportamento desejado	2	2	E1 - [...] Na verdade, isso é complicado de disseminar aqui dentro. É difícil isso, é uma parte da cultura. O único lugar que nós temos hoje é na política, é lá que está escrito. Então, se a pessoa ler, ela vai conseguir se comportar daquela forma. Se ela nem tomar conhecimento que aquilo existe ou tomar conhecimento e não ler, nós acabamos de perder um colaborador. A política está exposta na intranet, exposta a qualquer dia, a qualquer hora, sem prazo. [...]

Fonte: O autor (2014)

A pergunta 19, referente à variável **Treinamento, Capacitação e Conscientização**, discute a existência de programas de treinamento, capacitação e/ou conscientização periódicos na organização e suas influências no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação. Quanto ao emprego desses programas nas empresas pesquisadas, o Quadro 36 apresenta este resultado.

Quadro 36: Existência de Programas de Treinamento, Capacitação e/ou Conscientização no sentido de evitar Vulnerabilidades a Ameaças Internas

Existência de Programas	Frequência
Sim	9
Não	5

Fonte: O autor (2014)

Nove respondentes afirmaram a existência e a utilização de programas de treinamento, capacitação e/ou conscientização periódicos relativos à Segurança da Informação na organização onde trabalha, sendo que quatro não apresentam nenhum tipo dos programas relacionados. É importante ressaltar que na variável anterior foram avaliadas as formas de disseminação do comportamento responsável, na qual somente quatro afirmaram o uso de treinamentos e programas relativos à Segurança da Informação. Provavelmente, essa diferença se deve pelo fato de que os gestores entrevistados não consideram esses programas como uma forma efetiva de exposição do comportamento desejável a fim de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação.

Em relação à influência destes programas no sentido de evitar ou proteger contra vulnerabilidades a ameaças internas de Segurança da Informação percebida pelos gestores, o Quadro 37 resume esta informação.

Quadro 37: Influência da variável Treinamento, Capacitação e Conscientização na Proteção Contra Vulnerabilidades a Ameaças Internas de Segurança

Influência Percebida	Frequência
Sim	12
Não	2

Fonte: O autor (2014)

Como se pode observar, 12 entrevistados **confirmaram** a relação de influência dos programas de treinamento, capacitação e conscientização na proteção contra vulnerabilidades a ameaças internas de Segurança, com somente duas respostas negativas. É necessário salientar que o número de gestores que responderam positivamente à influência percebida foi maior do que o número que confirmou a presença destes programas na empresa onde trabalha. Isto se deve ao fato de que, mesmo não existindo treinamentos ou programas relacionados na organização, estes gestores acreditam que, com a utilização dos programas, a proteção contra vulnerabilidades a ameaças internas da Segurança da Informação seria maior.

As categorias mais citadas pelos respondentes nesta variável foram: **Evidências de relação entre programas e diminuição de vulnerabilidades** e **Pretensão de implantar programas de treinamento, capacitação e conscientização**. A categoria Evidências de relação entre programas e diminuição de vulnerabilidades, que obteve 11 citações e evidências, diz respeito à influência positiva dos programas de treinamento, capacitação e/ou conscientização na redução de vulnerabilidades a ameaças internas de Segurança. Para

justificar e ilustrar a categoria definida, o relato do Gestor I explica o funcionamento das etapas de treinamento na sua organização:

> [...] Desde que o funcionário chega, que é o momento em que ele começa a trabalhar, ele tem esse treinamento que nós chamamos de integração, que é tudo, desde como ele tem que fazer uma solicitação de reembolso de viagem, como ele tem que usar o computador dele, que ele não deve deixar o computador no carro quando ele fizer atendimento. Enfim, essas orientações. E assim, o que eu posso dizer é que, como nós temos um nível baixo de incidentes, de alguma forma, eu acredito que isso tenha relação. Não existe um indicador exato para isso. Nós temos dois indicadores. Nós temos a questão dos treinamentos, as metas de treinamentos que nós temos anualmente. E nós temos os indicadores de incidentes de Segurança internos. O que eu posso dizer é que nós não aumentamos o número de treinamentos. Nós temos treinamentos esporádicos, periódicos, normalmente duas vezes por ano, então você tem integração e mais dois, um a cada semestre, que nós fazemos um encerramento e uma orientação em todo o grupo. Mas nós estamos, ano a ano, reduzindo os incidentes. Então, os incidentes diminuem e os treinamentos existem [...]

Para o Gestor E, a diferença é notável entre ter ou não ter programas desse tipo:

> [...] Antes de nós termos isso lá na empresa, nós não tínhamos essa política e, antes disso, essa forma de comunicação, divulgação e reforço. Nós somos auditados, a nossa auditoria, periodicamente, avalia se a versão da nossa política está atualizada, se todo mundo sabe, eles fazem auditoria para ver se as pessoas conhecem a política. Então, para nós, isso nós botamos na rotina, no processo de melhoria contínua de Segurança da Informação. Antes disso, nós tínhamos muito problema de Segurança da Informação. Hoje, diminuiu quase a zero. [...]

O Quadro 38 mostra todas as categorias verificadas nesta variável e outras informações relevantes.

Quadro 38: Categorias da variável Treinamento, Capacitação e Conscientização

Categorias	Frequência	Total de Evidências	Outras Evidências
Evidências de relação entre programas e diminuição de vulnerabilidades	11	11	E4 - [...] certamente tem uma influência, pois se não existissem esses programas, as pessoas estariam menos informadas e, consciente ou inconscientemente, estariam mais propensas a ações que vão contra a política. [...] E9 - [...] tem relação, sim. É uma questão de educação, tem relação à questão dessas iniciativas de capacitação com a exposição de vulnerabilidades. A pessoa, a partir do momento que ela conhece melhor a disciplina, que ela começa a interagir com a disciplina de Segurança, os problemas tendem a diminuir. [...] E11 - [...] Quanto à relação dos programas de capacitação na exposição de vulnerabilidades, eu acredito que possa haver alguma relação, que esses programas ajudam a diminuir a exposição de vulnerabilidades ou brechas. [...]
Pretensão de implantar programas de treinamento, capacitação e conscientização	3	3	E3 - [...] Atualmente, nós não temos programas de treinamento e capacitação periódicos, mas estamos querendo implementar. Eu mesmo já fiz um planejamento de como fazer esse treinamento de conscientização e apresentei para a diretoria [...]
Tratamento reativo de eventos de Segurança da Informação	2	2	E1 - [...] hoje, a gente faz isso muito quando acontece um evento. A gente vai lá e trata o evento, seja ele como orientação, seja uma auditoria para tentar investigar e descobrir o que gerou determinado evento, mas é de forma muito reativa. [...]
Segurança da Informação como processo contínuo	2	2	E1 - [...] Principalmente, sempre que acontece uma ameaça e onde foi, nós vemos, revemos o processo, vemos onde nós falhamos, por exemplo, na política ou na capacitação das pessoas, para tentar melhorar. É um processo contínuo. [...] E2 - Então, fazemos de seis em seis meses para tentar sempre dar uma acordada e trazer o assunto de volta. E as próprias vulnerabilidades mudam também, um dia é de uma forma, outro dia é de outra. [...]
Maior conscientização após sanção sofrida por algum funcionário, porém com pouca duração	1	1	E1 - [...] na verdade, o que tem mais impacto é quando alguém daquela unidade sofre algum tipo de sanção em função de algum uso indevido, aí o pessoal se comporta, mas isso dura pouco. [...]
Temporalidade da conscientização relacionada com programas de treinamento, capacitação e/ou conscientização	1	1	E1 - [...] essa preocupação dura momentos, digamos um mês, dois meses, tem um ciclo. Ficam com aquilo na cabeça, levam isso até para casa e chegam depois aqui com dúvida. "Mas em casa, minha filha está fazendo isso, acessando aquilo, será que pode, será que não pode, o que eu devo fazer?" Mas nós vemos que, depois de um ou dois meses, aquilo se perde e voltam a ocorrer incidentes e casos. [...]
Pouca aderência dos funcionários aos treinamentos de Segurança	1	1	E1 - [...] certamente a empresa possui e-learning, tem treinamento virtual, mas era muito baixo o numero de participação. Esse ano nós tivemos 1200 pessoas que fizeram assinatura virtual de um total de 12000, 10% da organização. [...]

Fonte: O autor (2014)

A próxima variável a ser analisada é **Política de Segurança da Informação como Mecanismo de Proteção**, contemplada na questão 20 do roteiro de entrevistas, e aborda a Política de Segurança como um elemento satisfatório para evitar vulnerabilidades a ameaças internas de Segurança da Informação. Primeiramente, foi verificado se os gestores consideram que os colaboradores, seguindo somente a Política de Segurança da Informação, estarão contribuindo para a proteção da organização, o que é mostrado no Quadro 39.

Quadro 39: Política de Segurança da Informação como único mecanismo de proteção a fim de evitar Vulnerabilidades a Ameaças Internas

Atendimento somente da Política de Segurança da Informação	Frequência
Sim	9
Não	5

Fonte: O autor (2014)

Segundo a maioria dos entrevistados (nove ocorrências), o atendimento exclusivo da Política de Segurança da Informação pelos empregados **colabora** para a proteção contra vulnerabilidades a ameaças internas. No entanto, cinco respondentes negaram essa afirmação, dizendo que somente o cumprimento da Política de Segurança não basta para manter um ambiente relativamente seguro.

Como categoria melhor qualificada de acordo com a frequência de observações, temos a **Suficiência da política de Segurança da Informação como única proteção**. Com oito citações e evidências relatadas, ela trata como aceitável a utilização da Política de Segurança da Informação como forma exclusiva de proteção, situação relatada pelo Gestor I:

> [...] No caso da nossa empresa, sim. Porque ela é bem completa, contempla tudo que nos importa de comportamento. Mas isso não é o que nós vemos na prática, no ambiente corporativo. Hoje, na nossa empresa, por exemplo, existem diversos tipos de políticas, existem políticas educativas, existem políticas de normativas, políticas especialistas, que nós chamamos, por exemplo, somente para o uso de e-mail. Então, hoje, nós temos um conjunto de políticas que nos contempla, não vou dizer 100%, mas tudo que é vital para o nosso negócio. [...]

Conforme a visão do Gestor J, toda a Política de Segurança deveria fornecer o suficiente em termos de proteção contra vulnerabilidades de Segurança da Informação para a organização: “[...] Deveria. A política de Segurança deveria ser suficientemente abrangente para que o funcionário, somente seguindo o que está na política, ele esteja diminuindo a exposição da empresa a qualquer tipo de risco ou vulnerabilidade, enfim. [...]”

Em contraponto com a categoria anterior, a outra categoria mais citada foi **Insuficiência da política de Segurança da Informação como única proteção**. Com seis observações e evidências, diz respeito à incapacidade da Política de Segurança como exclusiva forma de proteção. O comentário do Gestor H observa a partir desse ponto de vista, afirmando que são necessários outros itens, juntamente com a Política de Segurança, para tornar efetiva a proteção contra vulnerabilidades a ameaças internas:

> [...] Só a política, não. No meu entendimento, só a política não basta para conseguir realmente dizer que eu estou seguro, que não existe brecha. A nossa política não é uma política pobre, é uma política que até tem certo grau de maturidade, já foi vista, revista, revisada. Mas acredito que só esse mecanismo, política de Segurança, não é uma forma correta de tentar fechar brechas e vulnerabilidades. [...]

A terceira categoria mais significativa, conforme as citações, foi **Comportamento e conscientização dos funcionários como fatores críticos para a Segurança**. Com cinco observações e mesmo número de evidências descobertas, ela aborda o comportamento responsável e a conscientização dos colaboradores como elementos indispensáveis para garantir a proteção contra vulnerabilidades a ameaças internas de Segurança da Informação. Conforme a abordagem do Gestor J, o comportamento e a conscientização são de extrema importância para a Segurança da Informação e devem estar contidos na Política de Segurança da organização, situação que não é habitual nas empresas:

> [...] O que ocorre é que nem sempre as empresas, saindo da nossa esfera aqui, têm uma política suficientemente abrangente. Então, neste caso, não contribuiria nesse sentido, porque a política não menciona casos que nós sabemos que são críticos, principalmente relacionado mais ao comportamento das pessoas assim. Não aqueles casos de que tem que ter controle de autenticação disso, que tem que ter determinadas ferramentas de Segurança ou processo para criptografia aqui e ali. Mais aquilo que depende das pessoas, da pessoa, por exemplo, não comentar sobre informações confidenciais em lugares públicos ou da pessoa fornecer informações via telefone, divulgar senhas entre setores, esse último até não é muito comum. O que eu vejo maior risco, maior vulnerabilidade associada, é a questão da pessoa acabar falando coisas que ela não deveria falar, seja por telefone, seja em local público, ela não está consciente de que pode estar expondo a empresa a situações de vulnerabilidade. Mas, se a política tiver suficientemente abrangente, ela vai abordar esse ponto, e esse é um dos pontos, como eu estava conduzindo esse trabalho internamente, é um dos pontos em que eu mais bato forte internamente, que é a questão desse tipo de coisa, da pessoa ter ciência de que, seja por qualquer meio, seja por telefone, local público, qualquer coisa. Você tem que saber o que pode falar, o que você não pode, precisa tomar cuidado quando tiver em lugar mais público, seja em utilizar o notebook em aeroporto, em avião, que as pessoas acabam usando e se esquecem que tem um monte de pessoas na volta enxergando o que elas estão fazendo ou usar uma rede que não é segura. Então, é mais nesse sentido. [...]

Todas as categorias descobertas nesta variável, assim como as observações, o número de evidências e outras evidências propriamente ditas estão disponíveis no Quadro 40 a seguir.

Quadro 40: Categorias da variável Política de Segurança da Informação como Mecanismo de Proteção

Categorias	Frequência	Total de Evidências	Outras Evidências
Suficiência da política de Segurança da Informação como única proteção	8	8	E3 - [...] Sim, somente atendendo a política ele estará contribuindo. Se ele atender a política e atender todos os outros processos da empresa, ele estará contribuindo mais. Mas só a política ele já estará contribuindo para evitar vulnerabilidades. [...] E8 - [...] Se esta política abranger todos os aspectos considerados de risco para a empresa, ou seja, ela estiver completa, sim. [...]
Insuficiência da política de Segurança da Informação como única proteção	6	6	E5 - [...] Então, somente a política não é tudo. Tem uma série de outros componentes que são importantes. A política dá o norte, mas tem outros componentes de comportamento, de atitude, de iniciativa, que contribuem nesse sentido. [...] E6 - [...] Então, eu te diria que não basta ele entender e atender a política de Segurança, não. [...]
Comportamento e conscientização dos funcionários como fatores críticos para a Segurança	5	5	E4 - [...] A política é um documento que rege as ações, as atitudes, as atividades, as iniciativas, mas tem uma série de comportamentos que não estão intrínsecos na política, de como a pessoa deve agir, falar, se comunicar em determinadas situações que contribuem muito por questões de Segurança e isso nem sempre está disponível num documento. [...]
Necessidade de atualização contínua da política de Segurança da Informação	3	3	E1 - [...] na experiência do dia a dia, você vai identificando soluções que poderiam ser tratadas e aí passam pelo plano de melhoria e você atualiza lá o teu plano de Segurança da Informação. [...]
Bom senso em situações não previstas na política de Segurança da Informação	1	1	E1 - [...] acho que vai muito do bom senso também, de situações que talvez não estejam previstas na política de Segurança da Informação e que podem futuramente ser incluídas ali. [...]
Engenharia social como fator crítico para a Segurança	1	1	E1 - [...] nenhuma empresa está preparada para lidar com uma situação de engenharia social. Eu não vejo isso. [...]
Falta de abordagem comportamental na política de Segurança da Informação	1	1	E1 - [...] Até porque na política de Segurança da Informação nós não fazemos, aí eu falo pela nossa empresa, talvez esteja errada, mas nós não focamos em ações comportamentais do usuário, nós focamos em ações, não em perfil comportamental, nós focamos na questão técnica, o que pode e o que não pode fazer, mas não em como pode ou não pode se comportar fora de um equipamento de TI. [...]

Fonte: O autor (2014)

A questão 21, que traz como tema a variável **Juízo de Comportamento Relacionado à Política de Segurança da Informação**, retrata o que se espera do colaborador em relação à Política de Segurança, se o funcionário deve realizar somente o que a Política permite ou se aquilo que não foi descrito na Política e que foi concretizado pelo empregado pode ser considerado adequado. No Quadro 41, é apresentada a percepção dos gestores frente a essas duas situações descritas na vigésima primeira pergunta do roteiro de entrevistas.

Quadro 41: Juízo de Comportamento Responsável Relativo à Política de Segurança da Informação a fim de evitar Vulnerabilidades a Ameaças Internas

Juízo de Comportamento Responsável Relativo à Política de Segurança	Frequência
Nenhuma das situações	9
Somente o permitido na Política	3
Situações fora da Política consideradas adequadas	2

Fonte: O autor (2014)

A partir da visão de nove entrevistados, **nenhuma** das duas situações descritas na questão 21 foi considerada relacionada com a proteção contra vulnerabilidades a ameaças internas de Segurança da Informação, o que revela a necessidade do entendimento ou do cumprimento de outros aspectos além dos contidos em uma Política de Segurança da Informação.

Entre as categorias expostas pela interpretação dessa variável, podemos relacionar as seguintes: **Avaliação individual de cada caso específico realizado que não consta na Política de Segurança da Informação**, **Necessidade de atualização contínua da política de Segurança** e **Defasagem da política de Segurança da Informação**. Com 11 citações e 14 evidências localizadas, a categoria Avaliação individual de cada caso específico realizado que não consta na Política de Segurança da Informação versa sobre a análise particular feita de acordo com cada situação diferente consolidada pelo colaborador que não esteja descrita na Política de Segurança. O Gestor F pondera que a consequência de algo realizado e que a Política não está abrangendo pode variar conforme os valores e princípios da organização:

> [...] A empresa não espera que o funcionário faça somente o que está expresso na política, mas é claro que o peso disso, a consequência de alguma coisa que não está na política, vai ser analisado de forma diferente, principalmente porque tem muitas questões da política que ainda estão em formação, que não tem uma regra clara, então se alguém tomou uma ação que não está escrito na política, bom, então vamos ter que parar primeiro e decidir. Isso realmente é uma coisa que vai contra os princípios da empresa ou não? Tem que decidir isso. E depois, conforme isso, aí pode ser que isso realmente não vai contra, isso não está na política, mas não se pode considerar que isso vai contra os valores ou princípios da empresa, então, como conseqüência, talvez se vá criar uma regra para explicitar isso, que isso é permitido. Ou isso não está escrito na política de forma clara, mas isso é uma coisa que vai contra os princípios e os valores da empresa, vai contra o código de ética, então realmente podemos considerar que a pessoa está tomando uma ação que está prejudicando a empresa e então vai ter uma outra consequência. Depende muito do julgamento daquilo que está escrito. [...]

Para o Gestor K, a análise de cada caso varia de acordo com a intenção do colaborador em ajudar a melhorar a Política de Segurança ou em apenas violar para obter benefício próprio:

> [...] Bom, como nós estamos sempre tentando fazer a evolução da política, sempre tentando trazer serviços novos, sempre tentando regularizar serviços de internet, muitas vezes, então se entende que, quando o funcionário tenta ou faz alguma coisa que não está na política, se for entendido que é para agregar, está certo. Se for entendido que ele fez isso de uma maneira, simplesmente, de trespassar a política para fazer alguma coisa que não deveria, fazer download de conteúdo protegido, ficar disseminando vírus ou spam, aí não, aí se entende que é errado. [...]

A segunda categoria mais citada, chamada de Necessidade de atualização contínua da política de Segurança, verifica que é preciso revisar periodicamente a Política de Segurança. Com seis observações e sete evidências descobertas, essa categoria pode ser ilustrada na fala do Gestor F, que avalia a atualização da Política de Segurança como uma maneira de se manter relativamente protegido frente ao dinamismo do cenário empresarial:

> [...] Considera-se adequado também o que não está contemplado na política. É uma questão que vem dos valores da empresa, e a política nunca vai conseguir expressar tudo o que existe, pois o mundo também é dinâmico, as coisas também mudam, algumas coisas na política, a política como parte das regras dentro da moral da empresa, mesmo algumas coisas que estão escritas hoje, amanhã pode ser que não sejam verdades. Ela não é eterna, ela tem que sofrer constantes revisões. [...]

Para o Gestor G, a Política de Segurança está sempre em atualização e, conforme o caso, já deve estar atualizada na próxima revisão:

> [...] Depende, a política tem um ciclo de PDCA muito grande. Ela sofre sempre atualizações. Então, eventualmente, alguma coisa que foi feita e que nós podemos adequar. 'Olha, isso poderia estar na política e não está'. Nós trazemos para a política e publicamos. Ela está sempre sofrendo atualizações. Então, alguma coisa que hoje não está na política e que pode ser adequado, e talvez não seja tão complicado, passa a ser política daqui uma próxima versão. [...]

A última categoria melhor classificada quanto ao número de observações foi Defasagem da política de Segurança da Informação, com quatro citações e cinco evidências encontradas. Retratando uma lacuna temporária que a Política de Segurança tem entre suas regras e a próxima revisão ou atualização, o Gestor M afirma resignadamente que sempre existirá situações que não foram previstas na Política: "[...] Então, a política de Segurança da Informação prevê aqueles casos conhecidos ou os casos imagináveis. Evidente que tem situações que podem vir a acontecer e que não estão previstas naquela política [...]".

Disposto logo a seguir, o Quadro 42 resume as categorias encontradas e outras informações relevantes na análise de conteúdo dessa variável.

Quadro 42: Categorias da variável Juízo de Comportamento Relacionado à Política de Segurança da Informação

Categorias	Frequência	Total de Evidências	Outras Evidências
Avaliação individual de cada caso específico realizado que não consta na Política de Segurança da Informação	11	14	E3 - [...] O fato é o seguinte, eu não posso penalizar como se estivesse previsto em lei, tem que avaliar cada caso. Por isso que a gente acaba querendo, se dispondo à disposição dos colaboradores. [...] E8 - [...] Na verdade, na política geralmente tem um item sobre isso, casos não contemplados aqui serão analisados por uma comissão com o pessoal de TI, RH, e tudo mais. [...] E10 - [...] Bom, se for alguma coisa completamente contra a política, ele está fora do modelo. Agora, se for alguma coisa que possa acrescentar à política, nós iremos trabalhar. A análise é de caso a caso. [...] E14 - [...] para um caso fora da política, ele tem que ser analisado e julgado para depois atualizar a política. [...]
Necessidade de atualização contínua da política de Segurança	6	7	E5 - [...] A política não é fixa, ela vai se moldando de acordo com as necessidades do negócio, com situações práticas que, eventualmente, acontecem. [...] E7 - [...] Posteriormente, depois do caso ter sido avaliado pelos gestores ou diretores, ele deve ser incluído na política, para deixar a política mais atualizada. [...]
Defasagem da política de Segurança da Informação	4	5	E1 - [...] Mas é um ponto complicado, porque é que nem a questão da Segurança. A política está sempre atrás das coisas novas. [...] E3 - [...] nunca vai se conseguir expressar o momento ou tudo que importa para aquele momento dentro da política, vai expressar somente uma parte disso. [...]
Suporte em caso de dúvida relacionada à política de Segurança	2	2	E1 - [...] Eu não posso considerar que ele tenha infringido uma norma, nem necessariamente concluir que tenha sido adequado. Por isso que a gente acabou colocando: "na dúvida, entre em contato com a Segurança da Informação". Ou: 'ligar nos nossos contatos'. [...]
Questões comportamentais contempladas no código de ética e nos valores e princípios da empresa	2	2	E2 - [...] a pessoa tem que ter base para isso, tem que ter base nos valores da empresa e os valores tem que orientar a ação dela dentro da empresa. E tem outros mecanismos também como o código de ética da empresa, que também vai dar orientações à pessoa naquilo que não está expressamente declarado na política, se aquilo é correto ou não. [...]
Política de Segurança da Informação como diretriz principal	2	2	E2 - [...] Mas sempre lembrando que a política é a base de tudo. O funcionário deve fazer tudo que a política manda, não deve quebrar regras. [...]
Proibição de situações não contempladas na política de Segurança	1	2	E1 - [...] Na nossa política, nós falamos que qualquer situação que não esteja suficientemente expressa, ela é proibida. [...]
Falta de bom senso dos funcionários	1	1	E1 - [...] Só que assim, o cara tem que ter bom senso. Se o MSN é bloqueado, o Facebook é bloqueado, o Orkut é bloqueado, porque que o Twitter estaria disponível? Só que aí depende do bom senso. Aí, daí esquece. Para isso, o pessoal não tem bom senso. [...]
Política de Segurança da Informação como difusora do que não é permitido	1	1	E1 - [...] Na verdade, a política diz mais o que ele não pode fazer. [...]

Fonte: O autor (2014)

A variável **Seriedade da Violação de Regras e Normas**, correspondente à vigésima segunda pergunta do roteiro de entrevistas, afirma que qualquer violação de regras e normas é algo muito sério e deve ser tratado com punição, independente de qualquer outro fator envolvido. A seguir, o Quadro 43 apresenta a percepção dos gestores frente a essa questão.

Quadro 43: Seriedade da Violação de Regras e Normas no sentido de proteger contra Vulnerabilidades a Ameaças Internas

Seriedade das Violações	Frequência
Sim	8
Não	6

Fonte: O autor (2014)

Com oito respostas afirmativas dos entrevistados, a violação de regras e normas foi **considerada** uma questão séria e que merece punição, a fim de evitar vulnerabilidades a ameaças internas de Segurança da Informação. No entanto, seis gestores responderam negativamente a essa pergunta, o que pode estar relacionado ao fato de que nem todos considerem a punição como melhor forma de lidar com uma transgressão ou, ao menos, não em casos de incidentes de Segurança considerados de baixa gravidade ou não intencionais.

A categoria com maior número de citações nesta variável foi **Punição de acordo com a gravidade do caso**, com oito observações e evidências. Ela aborda a ideia de que a penalidade deve variar conforme a gravidade da violação realizada pelo empregado, fato que pode ser observado no relato do Gestor F, que mostra os extremos de uma punição:

> [...] Sim, merece sempre que seja observado. Eu não vou dizer punição. Punição, em alguns casos. Em outros, pode ser um aviso ou uma advertência. Sempre que uma pessoa viola uma regra vai desde um: “olha, isso aqui é uma coisa que não se pode fazer dentro da empresa por esse e aquele motivo, talvez você não esteja ciente, isso vai expor a empresa dessa e dessa outra forma”. Vai desde um aviso desses, um aviso amigável, vamos a extremos, desde um aviso amigável até uma demissão por justa causa. Um outro extremo, o mais extremo de todos, até em alguns casos, além disso, até um processo formal na justiça, pegando casos extremos. Mas depende do caso, enfim. [...]

Já o Gestor J ilustra diferentes casos onde a punição deve ser diferenciada:

> [...] Depende. Por exemplo, determinadas situações de violação nós temos que tratar de uma forma um pouco diferenciada. É diferente a punição, por exemplo, por eu deixar o meu computador desbloqueado quando eu saio da frente dele do que eu, por exemplo, passar senha para um colega, compartilhar senha com um colega ou passar senha por telefone para outra pessoa acessar um recurso que é de minha responsabilidade. É completamente diferente. Então, não concordo que não importa. Eu acho assim, para diferentes situações, exige punições diferenciadas. [...]

Para o Gestor M, de acordo com sua visão, a punição deve ser feita com base na intenção que o colaborador teve ao violar uma regra ou norma:

> [...] Punição é um pouquinho forte, a punição entenda-se desde uma advertência até, enfim, alguma ação. É um assunto sério, sim. A partir do momento da quebra da Segurança da Informação e, de novo, é um caso a caso. O cara pode quebrar e ter má índole ou o cara pode quebrar e não leu. Aqui é um exemplo que eu usei no início, que ele tem a política, ele sabe que tem a política, mas não conhece o conteúdo. Vou te citar um exemplo aqui. O usuário trouxe um HD de 3TB, espetou na máquina dele para copiar música para a máquina dele, ou seja, trouxe de casa música e copiou para a máquina dele. Ele está quebrando a política, mas não está tendo má índole no sentido de prejudicar a empresa. Por outro lado, você espetar o mesmo HD e fazer cópia inversa, não de música, mas de arquivos de dados, eu estou pegando um exemplo bem xucro, está ilustrando a má-fé do cara. Então, eu não estou minimizando o fato do cara ter espetado o HD, eu estou julgando a índole do usuário. Em teoria, a ação foi a mesma, o cara espetou um HD na máquina, mas a punição tem que ser diferente. Então, eu não acho que não deva ter. Respondendo a pergunta, a violação no primeiro exemplo foi muito pequena, no meu ponto de vista, mas não dá para deixar barato, tem que, pelo menos, ir lá e falar com o cara. No segundo caso, o cara vai ser desligado. Avaliação pontual de novo. [...]

A outra categoria mais citada desta variável foi **Treinamento, instrução e conscientização em caso de eventos de Segurança de baixo risco ou não intencionais**, com três observações e evidências. Assim, em incidentes de Segurança com baixo risco envolvido, despropositais ou sem pretensão, o treinamento, a instrução e a conscientização devem prevalecer frente à punição, situação descrita pelo Gestor B:

> [...] Na minha visão, assim, eu acho que não é qualquer regra que merece punição. Talvez tenham regras que precisem mais de treinamento e instrução do que punição. Já vi acontecer do pessoal do financeiro acessar o site do banco, deixar ligado o computador e ficar lá o extrato da empresa. O cara não fez por maldade. Ele não pode ser punido por isso da mesma forma que alguém que passou informações confidenciais para fora da empresa. Tem que ser tudo definido na política, não é. Pesos e medidas bem claros. Eu acho que existem pesos e medidas, sim. A questão que for menor, vale mais a instrução do que uma punição. [...]

O Gestor E descreve um exemplo verídico em que um incidente de Segurança causado por um colaborador num momento de desatenção, o qual foi considerado não intencional, onde a orientação deve ser utilizada:

> [...] Eu acho que não deve ser punitivo, mas sim, orientativo. No primeiro momento, muitas vezes, por desconhecimento, nem todo mundo tem o profundo conhecimento de alguns temas em Segurança da Informação. Então, Segurança da Informação não é apenas aquela Segurança da Informação eletrônica de computador, mas também é essa. Nem todo mundo tem familiaridade com computador e muitas vezes tu pega um funcionário que não utilizava o computador, dá a capacitação, mas ele nunca usou o computador, não tem a familiaridade e, de forma não intencional, ele pode gerar um problema de Segurança da Informação. Vou dar um exemplo, uma pessoa da nossa organização foi promovida para o departamento de Recursos Humanos, foi trabalhar na área de Recursos Humanos. Ela trabalhava coletando o ponto, ponto eletrônico, e lançava na planilha Excel, e aí ela passou a usar o sistema de folha de pagamento dentro da empresa e um dia, sem querer, ela foi no sistema de folha de

> pagamento e gerou uma listagem de todos que tinha que pagar naquele mês, só que ela mandou botar na impressora e errou a impressora, e saiu na impressora de um outro andar. Saiu na impressora todos os salários de todos os colaboradores da empresa. Chegou uma pessoa externa, chamou todos os colegas e divulgaram para toda a empresa o salário de todos os colaboradores. Não foi intencional, porque a pessoa não queria ter feito, ela conhecia as regras e políticas, mas foi um descuido não intencional. E gerou um problema de Segurança da Informação porque vazou uma informação que não era para ter vazado da organização. [...]

Para fins de comprovação, o Quadro 44 apresenta todas as categorias encontradas na interpretação dos dados desta variável. Nele também constam informações como a frequência de citações, o número total de evidências e outros relatos dos gestores como forma de justificativa das categorias.

Quadro 44: Categorias da variável Seriedade da Violação de Regras e Normas

Categorias	Frequência	Total de Evidências	Outras Evidências
Punição de acordo com a gravidade do caso	8	8	E8 - [...] a punição depende do caso. Depende da violação que o cara fizer. Se rolar um vazamento de informação, algo que é agravante, a punição tem que ser diferente, mais pesada do que para um caso comum, leve. [...]
Treinamento, instrução e conscientização em caso de eventos de Segurança de baixo risco ou não intencionais	3	3	E3 - [...] Tem casos graves em que a pessoa é mal intencionada mesmo, mas muitos casos, que é a grande maioria, a imensa maioria, que é falta de cuidado, falta de informação. Aí nós não trabalhamos com punições, se trabalha com conscientização, com educação. [...]
Tendência de que eventos de Segurança não punidos resultem em outros eventos de Segurança futuramente	2	2	E1 - [...] Não interessa se tu estás baixando uma musica ou cinco CD's porque, no momento que tu não pune as pequenas, as pequenas viram grandes. [...] E2 - [...] Às vezes, as normas, as regras são quebradas e não se tem uma punição. No máximo, uma conversa ou algo do gênero, como eu tinha mencionado anteriormente. Isso acarreta novos incidentes, novas falhas, novas vulnerabilidades. [...]
Necessidade de controles e conscientização antes da aplicação de punições	1	1	E1 - [...] Acho que a punição faz parte, mas acho que, antes da punição, tu deve ter primeiro o controle e a conscientização, para depois ter a punição. [...]
Reatividade em relação à Segurança da Informação	1	1	E1 - [...] Em função de nós não termos conseguido identificar quem que fez essa atividade, foi comprado uma solução agora que tem todo o controle de atividade e monitoramento e hoje nós teríamos como dizer exatamente quem foi que executou, mas precisou acontecer o evento [...]
Punição em caso de reincidência de evento de Segurança	1	1	E1 - [...] Agora, num segundo momento, uma repetição, sim, tem que ter meios punitivos quanto a isso. A reincidência para mim deve ser punitiva, a incidência não. [...]
Consequência de um evento de Segurança para o funcionário como forma de exemplo	1	1	E1 - [...] Mas tem uma consequência, seja ela a mais branda até a mais pesada. É importante para mostrar que as regras, elas realmente valem, e que elas estão aí porque elas são importantes para manter a estabilidade da empresa. [...]
Uso de ferramentas de análise de incidentes de Segurança para facilitar o controle	1	1	E1 - [...] O que nós orientamos é trazer tecnologias que nós chamamos de análise de correlação de eventos, de análise comportamental de incidentes de Segurança, e é isso que nós fazemos na nossa empresa. [...] Então você tem um incidente específico de Segurança, pequeno, ele não precisa ser tratado, mas quando existe uma relação entre vários pequenos incidentes de Segurança que podem gerar um incidente maior, você tem uma ação. [...]
Classificação dos tipos de violação na política de Segurança para facilitar a definição da punição	1	1	E1 - [...] definam o que é uma violação leve, média e alta, que daí fica fácil definir a punição para isso. Se não tiver essa definição, às vezes, fica muito subjetivo tomar uma decisão de como punir determinado comportamento. [...]

Fonte: O autor (2014)

Continuando a análise das variáveis, temos a variável **Prejudicialidade da Violação de Regras e Normas**, relacionada à questão 23. Por meio da afirmação de que regras e normas podem ser violadas desde que ninguém seja lesado, o Quadro 45 mostra a percepção dos respondentes no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação.

Quadro 45: Prejudicialidade da Violação de Regras e Normas no sentido de proteger contra Vulnerabilidades a Ameaças Internas

Prejudicialidade das Violações	Frequência
Não	13
Sim	1

Fonte: O autor (2014)

Conforme a percepção da maioria dos entrevistados (13 gestores), não se deve violar regras e normas mesmo que ninguém seja prejudicado. Um único respondente afirmou ser possível violar regras desde que ninguém seja lesado, a fim de proteger contra vulnerabilidades a ameaças internas de Segurança.

Quanto às categorias mais significativas desta variável, a primeira mais citada foi **Qualquer violação de regras e normas é prejudicial**, com sete observações e oito evidências relacionadas. Considerando toda e qualquer violação de regras e normas como algo que possa causar dano, é possível identificar nas palavras do Gestor D que sempre a organização, de alguma forma, será prejudicada:

> [...] Na verdade, tu sempre estás prejudicando. Se a regra existe, é porque, em algum momento, aquilo pode prejudicar. O cara estuda na PUC e resolveu baixar o PowerPoint da aula de amanhã. Não está prejudicando ninguém, a princípio, porque o material lá na faculdade é publico, é para educação, não tem nada a ver com pornografia e não tem nada a ver com vírus, mas aquele arquivo tem um volume e aquele volume vai usar todos os recursos da empresa para chegar até a maquina dele, ou seja, ele vai usar a nossa internet, vai usar todos os servidores de proxy, servidor interno, ate chegar na máquina dele. Na máquina dele, provavelmente, ele vai deixar uma cópia, vai copiar no pen drive e vai levar para faculdade, ou seja, isso tudo tem um custo. Tem o custo da banda de internet, da rede local e tudo mais, que tu tens e que não foi dimensionado para isso. Até nesse último e-mail que a comunicação interna mandou e que eu fiz o texto junto com o pessoal do RH, no final, diz assim: “não é de expectativa da empresa suprir a necessidade de entretenimento, comunicação ou interação social dos funcionários com os recursos disponibilizados, não é essa a expectativa da empresa, os recursos estão aqui para serem usados em prol da empresa, para obtenção de lucro da empresa”. É isso. Isso gera uma série de discussões, por exemplo, uma vez deu um problema em relação a isso, o cara tava baixando um monte de material da faculdade, se nós estamos em Porto Alegre, muitas vezes pode até não ter sentido porque aqui nós temos um link grande, todo mundo está direto na intranet, tem o bloqueio igual, mas está direto. Mas uma unidade, por exemplo, Montes Claros, no interior de Minas Gerais, ele tem um link de 512K, aqui a gente tem um link de 10MB para a internet, o cara começou a

> baixar o material da faculdade dele lá e travou o link porque ele começou a baixar e não se deu conta que todas as outras aplicações estavam parando. A gente falou: “cara, não faz isso”. “Ah, mas a empresa até paga parte da minha faculdade pelo programa de incentivo, ela paga para eu fazer e eu não posso baixar os negócios na empresa?” “Não, não pode. São coisas completamente diferentes”. Então, é complicado. Mas mesmo não prejudicando ninguém, de alguma forma indireta, prejudica a empresa. [...]

A segunda categoria mais citada foi **Qualquer violação de regras e normas é inaceitável**, com três observações e evidências, e aborda a transgressão de qualquer regra ou norma como algo intolerável para a gestão da Segurança da Informação e para a organização. Conforme a visão do Gestor A para esta situação, as regras e normas já são de pouca intensidade e a violação delas seria inadmissível:

> [...] Então, no meu entender, não pode. E nós somos muito brandos nas nossas políticas ainda, não é. Mas dentro dessas políticas, se elas forem quebradas na empresa, vai ter algum tipo de punição à pessoa que fizer. A empresa não tolera esse tipo de coisa. Então, se tem a regra lá, ela pode ser branda, mas se o cara, por alguma razão, ele não cumpriu aquela regra, ele burlou aquela regra, foi identificado, ele vai ser, no mínimo, notificado, vai levar algum tipo de advertência e, dependendo da criticidade, ele pode até ser desligado da empresa. Mas a nossa posição, da TI e da empresa, é que isso é inaceitável. Já é bastante brando, não é. Aí o cara abusa. [...]

A terceira categoria classificada, de acordo a frequência de observações e o número de evidências, foi **Qualquer violação de regras ou normas pode expor risco à empresa**, com o mesmo número de citações e evidências da categoria anterior. Considerando qualquer infração de normas ou regras uma grande chance de estar suscetível à exposição de riscos para a organização, a descrição do Gestor F caracteriza perfeitamente esta situação:

> [...] Ou pode ser que não tenha uma ação que, às vezes, as pessoas confundem. É que se eu fizer isso, fiz isso e não aconteceu nada com a empresa. Só que a empresa não se preocupa com a consequência. Ela se preocupa com o risco. Não fez, mas existe o risco daquilo ter causado alguma coisa ou ter um efeito negativo na empresa. Então, o fato de você violar alguma regra, pode ser que não apareça, a empresa não perdeu nada do seu resultado, nenhuma outra pessoa foi prejudicada, mas o risco exposto foi alto. A preocupação da empresa é essa. Nem sempre é com uma ação concreta, mas é com o risco. O fato de você violar uma regra, no mínimo, você está expondo a empresa ao risco. Então, é prejudicial. [...]

No Quadro 46, estão disponíveis para apreciação todas as categorias definidas na análise, bem como diversas outras informações de interesse da pesquisa.

Quadro 46: Categorias da variável Prejudicialidade da Violação de Regras e Normas

Categorias	Frequência	Total de Evidências	Outras Evidências
Qualquer violação de regras e normas é prejudicial	7	8	E4 - [...] Não, não pode violar. O fato de existir regras, se as regras existem, é porque a empresa já entende que aquilo é prejudicial à empresa. [...] E7 - [...] Se existem regras é porque essas regras estão associadas a algum tipo de problema que a violação das regras possa acarretar. Então, se a regra for violada, se uma norma não for cumprida, alguém ou algo ou a instituição, vai ser prejudicado. [...]
Qualquer violação de regras e normas é inaceitável	3	3	E2 - [...] Eu acho que uma regra que é definida não pode ser burlada. [...] E3 - [...] independente de alguém ser prejudicado ou não, não pode haver violação das regras. [...]
Qualquer violação de regras ou normas pode expor risco à empresa	3	3	E2 - [...] Não é questão de ninguém ser prejudicado, é o nível do risco que pode comprometer. Pode não acontecer nada, mas o risco poderá existir. Pode não acontecer nada, mas está na política e pode ter acontecido algum risco. [...] E3 - [...] A ideia é que o problema não é que ninguém seja prejudicado, é que, às vezes, nós não temos a consciência de qual é o risco que está associado com aquele controle que foi definido na política. [...]
Explicação dos motivos das regras e normas para melhor entendimento	2	2	E2 - [...] O que nós orientamos nos programas de orientação é dizer qual o motivo de um determinado conteúdo ter sido implementado. Eu, pelo menos, quando eu dou palestra sobre isso, eu procuro expor dessa forma porque é mais fácil convencer a pessoa, dela entender porque ela está seguindo aquilo, do que só porque está escrito. [...]
Violação de regras e normas intencionais não são toleradas	1	1	E1 - [...] Agora, se ela tem a consciência de que existe essa norma e a pessoa burla, ela deve ser chamada para orientá-la que não faça mais aquilo ou identificar porque ela fez aquilo. [...]
Violação de regras e normas não intencionais são toleradas	1	1	E1 - [...] Pode burlar não intencional. "Ah, eu não sabia". Isso pode. [...]

Fonte: O autor (2014)

A última variável relacionada à dimensão Comportamento Responsável Relativo à Segurança da Informação, abordada na vigésima quarta pergunta, é a variável **Legitimidade da Violação de Regras e Normas**. A partir da consideração de que violar regras e normas pode ser permitido, desde que seja para obter melhor produtividade, todos os 14 gestores entrevistados responderam **negativamente** a essa questão, ou seja, quebrar regras e normas não é válido, nem que seja para aumentar a produtividade, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação.

Com sete citações e oito evidências relatadas, a categoria **Solicitação de mudança na política em casos onde a violação de regras e normas pode trazer melhorias** foi a mais

significativa desta variável. Em situações onde uma provável transgressão de regras e normas pode proporcionar melhorias nos processos da organização, o requerimento para alteração da Política de Segurança pode ser o melhor caminho, conforme revela o Gestor D:

> [...] Não. Na verdade não. O que tu tens que fazer? Se tu acha que tem alguma regra que impeça, que deixe o negocio mais lento e tudo mais, tu podes sugerir mudanças. Esse é o caminho certo. Tu não podes burlar, tu tens que pedir a alteração. Como se fosse um sistema legislativo. Na verdade, se tu não concordas com uma lei ou coisa assim, não adianta tu burlar a lei. Não é essa a solução. A solução é fazer o pedido para o setor legislativo e tudo mais para que a lei seja mudada. E se é de senso comum que ela tem que ser mudada, ela vai ter que mudar. Algumas regras que a gente tinha foram mudando à medida que foi tendo uma maturidade diferente e a gente tendo um entendimento melhor da situação. Algumas regras foram mudadas, ou seja, não é burlando a regra que tu fazes ela mudar. É comunicando nos locais adequados. [...]

Para o Gestor F, a evolução da Política de Segurança depende da percepção dos colaboradores no cotidiano da organização e da efetiva comunicação dessa percepção, o que pode ser notado no seu relato:

> [...] O funcionário pode sugerir alguma coisa em relação à política de Segurança e isso tem que fazer parte do processo de evolução desse conjunto de regras da empresa. Aí tem que ter os meios, as pessoas tem que ter um canal para falar isso. “Essa regra não concordo por isso e isso, acho que isso já passou, isso já está ultrapassado, isso aqui já não vale mais, isso já tem outras práticas melhores que essa”. Isso é fundamental para que isso não fique parado. Existe normalmente um conjunto de pessoas, um comitê, que trata a política e que precisa ser alimentado da visão que as pessoas estão tendo do dia a dia, porque no dia a dia que ela vai saber se aquilo realmente se aplica da forma como está escrito ou não. [...]

Como segunda categoria mais citada, **Revisão contínua da política para evitar violações das regras e normas** obteve quatro observações e quatro evidências denotadas. Segundo essa categoria, a atualização da Política de Segurança deve ser periódica ou então quando se há necessidade de revisão, com o intuito de impedir infrações de regras ou normas. Segundo o Gestor F, a Política de Segurança nunca está plenamente finalizada e sempre precisará de ajuste para evoluir:

> [...] O que existe muitas vezes são situações em que as regras podem conflitar entre elas. Pegando um exemplo fora daqui, num banco, para eu não cometer uma fraude, nesse caso, falando numa situação hipotética, eu vou precisar quebrar uma regra de Segurança. Então, isso deve ser julgado. Mas as regras estão aí justamente para isso, para que elas possam evoluir. E isso vai apontar que elas precisam ter algum ajuste entre elas, para que elas convivam melhor. Isso é constante, nunca elas vão estar terminadas, nunca vão estar 100% acertadas, porque o mundo também continua mudando.[...]

As novas vulnerabilidades, a evolução da tecnologia e o mercado de trabalho são motivos para manter a Política de Segurança da Informação em constante revisão, conforme pode ser notado na visão do Gestor H:

> [...] Sim, ela é adaptável, ela tem revisão. Se faz sentido, sim. Não vamos mudar toda uma política ou um parágrafo, que seja, e passar por aprovação de auditoria e diretores, se não faz muito sentido. Mas quando nós percebemos que aquela ali é a melhor forma. E é como eu te falei, as vulnerabilidades, não só as vulnerabilidades, a tecnologia e essa tendência de mercado fazem com que nós tenhamos que mudar a política. Digamos que na política de três anos atrás, redes sociais era proibido aqui dentro. Hoje, nós não podemos escrever isso na política, porque pode aqui dentro. Então, você tem que ir de acordo com o mercado e ir ajustando. [...]

Para ilustrar todas as categorias verificadas nesta variável, o Quadro 47 dispõe outras evidências relevantes como uma forma de melhor caracterizar a análise.

Quadro 47: Categorias da variável Legitimidade da Violação de Regras e Normas

Categorias	Frequência	Total de Evidências	Outras Evidências
Solicitação de mudança na política em casos onde a violação de regras e normas pode trazer melhorias	7	8	E5 - [...] Caso alguém descubra algo que possa melhorar a produtividade sem afetar a Segurança, existem duas formas: ela pode falar com o superior direto dela, o gestor dela, e sugerir essas melhorias, isso, às vezes, acontece; ou ela pode até registrar isso, notificar como um incidente de Segurança, sugerindo uma melhoria. [...] E8 - [...] se você acha que pode aumentar a produtividade, então você tem que discutir a política com alguém e não quebrar as regras. Pega a política e leva ali. Não quebra a regra. Se questiona, canal aberto. É avaliado. [...]
Revisão contínua da política para evitar violações das regras e normas	4	4	E1 - [...] a norma, claro, tem que ser sempre revisada, porque também, às vezes, as coisas em volta dela vão mudando e a norma fica parada. Então, de tempos em tempos, ela tem que ser adaptada. [...]
Aumento do risco em caso de qualquer violação de regras e normas	3	3	E1 - [...] a pessoa sempre tenta burlar o procedimento e tenta fazer de um jeito mais rápido e simples, mas daí mais sujeito ao risco. [...]
Política de Segurança adaptada ao negócio para ter produtividade	2	2	E1 - [...] Tu deves ter uma política que reflita isso. Não é justificativa e sim deve haver um modelo de gestão no qual seja flexível o suficiente ou ágil o suficiente para poder entender as linhas de negócios, avaliando os riscos e mantendo os controles necessários. [...]
Punição em casos de violação de regras e normas para obter produtividade	1	1	E1 - [...] se a pessoa, por conta própria, burlar a regra para aumentar a produtividade e, daqui a pouco, ela se destacar em relação a outras, ela vai ser tratada conforme o item anterior. Burlou a regra, é passível de punição. [...]
Excesso de criatividade do brasileiro favorece a violação de regras e normas	1	1	E1 - [...] A gente nota muito no Brasil e não só na área de Segurança, mas em tudo que é área, porque o brasileiro, por tendência, é um pouco criativo demais. [...]
Existência de violação de regras e normas a pedido da alta administração	1	1	E1 - [...] As pessoas violam regras porque precisam fazer uma entrega, alguma coisa lá para a cúpula, para a diretoria, presidente e acabam burlando. [...]
Utilização do canal de notificação de incidentes de Segurança para sugestão de melhorias	1	1	E1 - [...] o que o pessoal acaba fazendo é utilizar o mesmo canal de notificação de incidentes para sugestão de melhorias. Seja notificar uma questão de fraude, seja notificar uma questão de incidente de Segurança ou até uma sugestão de melhoria. [...]

Fonte: O autor (2014)

Terminada a etapa de análise das variáveis integrantes da dimensão Comportamento Responsável Relativo à Segurança da Informação, passaremos para a interpretação das variáveis pertencentes aos Moderadores do Comportamento Responsável. A primeira variável a ser analisada, denominada **Gênero**, está relacionada com a questão 25 e trata a influência que o gênero dos colaboradores pode provocar no comportamento responsável relativo à Segurança da Informação. No Quadro 48, se pode observar a percepção dos gestores frente a este tema.

Quadro 48: Influência da variável moderadora Gênero no Comportamento

Influência Percebida	Frequência
Não	8
Sim	6

Fonte: O autor (2014)

Pela percepção de oito respondentes, o gênero dos colaboradores **não** influência no comportamento considerado adequado relacionado à Segurança da Informação. Entretanto, seis gestores afirmaram a possibilidade da existência de relação entre gênero e comportamento desejável. Pela proximidade dos resultados, estudos confirmatórios deverão ser realizados para atestar a veracidade desta relação.

A categoria melhor qualificada pelo número de frequências e evidências encontradas foi **Evidências de que mulheres têm comportamento mais responsável em relação à Segurança**, com cinco citações e evidências. Ela apresenta afirmações categóricas de que mulheres tendem a se comportar mais adequadamente do que os homens em relação à Segurança da Informação, o que pode ser verificado no comentário do Gestor A:

> [...] É, aqui eu coloquei a questão do gênero mais para separar porque eu acho que a mulher, a nossa impressão, na verdade, não existe um estudo científico sobre isso. Não medimos, não é. Mas o nosso sentimento é que as mulheres são mais conscientes dessas coisas do que os homens. “Vou clicar aqui, está dizendo que é a foto da fulana de tal, da última mulher do BBB, vou clicar para ver”. E as mulheres já são mais: “Não”. Mas isso é um sentimento, não é. Como eu disse, não existe nenhum. Não dá para medir realmente. Nos parece aqui, a experiência que a gente tem no dia a dia é que as mulheres são mais aderentes às políticas, mais consciente dos riscos e tudo mais, então eu coloquei gênero nesse sentido de que as mulheres gerariam menos. Na verdade, os homens aqui estão mais associados com vulnerabilidade. [...]

Na visão do Gestor D, mesmo que a minoria dos colaboradores seja do sexo feminino, é possível perceber uma tendência de que as mulheres se comportam mais responsavelmente frente à Segurança da Informação:

> [...] E a questão de gênero aqui, mulheres tem tendência de seguirem melhor, de ter um comportamento mais adequado em relação à Segurança da Informação. Não todas, mas geralmente, 80% dos casos que a gente tem são homens. Claro que tem muito mais homens trabalhando na empresa do que mulheres, mas, geralmente, elas se comportam melhor. A regra é igual para todos, mas, dificilmente, a gente tem e-mails indevidos enviados por mulheres ou acessos indevidos feitos por uma mulher. Eventualmente, tem, mas é muito raro. Homem é a grande maioria. [...]

No Quadro 49, disposto a seguir, estão todas as categorias encontradas nesta variável e outras evidências que servem para ilustrá-las.

Quadro 49: Categorias da variável Gênero

Categorias	Frequência	Total de Evidências	Outras Evidências
Evidências de que mulheres têm comportamento mais responsável em relação à Segurança	5	5	E2 - [...] Mulher, com certeza, tem mais consciência e é mais, digamos assim, reticente na hora. É mais fácil a mulher ligar para nós e perguntar do que se trata o e-mail ou se aquele conteúdo é realmente confiável do que os homens. "Eles vem e formatam a minha maquina aqui, a gente revisa aqui e já resolve". A mulher, não. Tem mais cuidado. [...] E5 - [...] a percepção que tenho é que a mulher é mais disciplinada. E eu falo não só na política de Segurança da Informação, mas por outros exemplos. Eu vejo que a mulher é muito mais detalhista. Ela faz muito mais documentação, ela atualiza documentação, ou seja, ela tem alguns cuidados que o homem, no meu ponto de vista pessoal, não tem. [...]
Evidências de que mulheres têm comportamento mais responsável em relação à Segurança na área de TI	1	1	E1 - [...] nós notamos que na área de TI, sim. As mulheres são completamente corretas, procuram seguir as regras, e os homens, não, estão sempre tentando burlar as regras, fazendo de alguma forma [...]

Fonte: O autor (2014)

A segunda variável moderadora do comportamento é **Lealdade à Empresa**, descrita na vigésima sexta pergunta do roteiro de entrevistas, e trata da relação de influência da lealdade e da fidelidade dos colaboradores com a organização no comportamento responsável relacionada à Segurança da Informação destes. Segundo a percepção de todos os 14 gestores entrevistados, a lealdade dos funcionários com a empresa **influencia** no comportamento responsável.

Com relação à categoria mais citada desta variável, temos: **Evidências de que funcionários leais têm comportamento mais responsável em relação à Segurança**. Com nove observações e evidências relatadas, esta categoria refere-se às afirmações de que empregados considerados leais à organização se comportam mais adequadamente frente à Segurança da Informação, o que pode ser notado na fala do Gestor K:

> [...] Um funcionário leal, um funcionário que entende o papel dele na organização e ele veste a camisa, trabalha para isso, se ele tem acesso a informações sigilosas, ele tem a barreira ética dele de passar essa informação para outra empresa. Por exemplo,

> eu tenho uma lista financeira e eu vou passar isso para outra empresa porque eles vão me pagar por isso. O funcionário leal não faria isso. Nós entendemos que ele quer, ele gosta da empresa, ele trabalha nela há tanto tempo, ele vai continuar aqui, ele veste a camisa, então ele não faz isso, isso é antiético. Um funcionário que não é leal, que não está satisfeito, às vezes, pode pensar nisso e esse tipo de situação tem que ser barrada nos processos de Segurança. [...]

Conforme o ponto de vista do Gestor H, os indivíduos que foram considerados leais pela sua avaliação são mais responsáveis, a ponto de não existir vulnerabilidades ou brechas: "[...] Pelo menos, na prática, no meu conhecimento, pelo dia a dia das pessoas, eu percebo que aquelas pessoas que eu, que cada um tem seu ponto de vista, considero leais, são as que mais respeitam a política. Logo, não existe brecha ou vulnerabilidade com essas pessoas. [...]"

Já para o Gestor L, o colaborador leal tem um comportamento mais responsável pois conhece e cumpre as regras e normas de Segurança da Informação:

> [...] Sem dúvida. O funcionário leal é aquele funcionário que conhece e cumpre as normas, as políticas corporativas. É a pessoa que é leal à empresa e que realmente trabalha de uma forma positiva. Ela vai ter um comportamento mais responsável no que diz respeito à Segurança, porque ela vai conhecer e ela vai cumprir as normas de Segurança. [...]

O Quadro 50 abaixo mostra as categorias definidas na análise de conteúdo, assim como a frequência de observações e outras evidências relevantes.

Quadro 50: Categorias da variável Lealdade à Empresa

Categorias	Frequência	Total de Evidências	Outras Evidências
Evidências de que funcionários leais têm comportamento mais responsável em relação à Segurança	9	9	E1 - [...] No ambiente organizacional, um funcionário leal certamente terá um comportamento mais adequado. [...] E2 - [...] O comportamento tem a ver com a lealdade. Cada pessoa vai ter um comportamento e esse comportamento é baseado no quão leal ele é com a organização. [...] E7 - [...] Quanto mais leal o funcionário for aos princípios da empresa, a tendência é que ele siga mais as normas de Segurança ou que adote um comportamento mais responsável em relação à Segurança. [...]
Lealdade de um funcionário à empresa não é determinante no comportamento responsável relativo à Segurança	1	1	E1 - [...] Eu já vi funcionários extremamente leais mexendo, por exemplo, no banco de dados da empresa porque eles queriam acelerar um caminhão que deveria sair do pátio com uma entrega, que eles iam tomar uma multa. Então, ele fez aquilo na melhor das boas intenções, mas ele tornou o banco inconsistente. Ele feriu uma série de aspectos de Segurança, integridade, coisa e tal. Então assim, eu acho que, na verdade, lealdade não é determinante. O cara pode ser leal e fazer grandes burradas em termos de Segurança. [...]

Fonte: O autor (2014)

A terceira variável moderadora do comportamento é Escolaridade, retratada na questão 27, que aborda o nível de escolaridade do colaborador como influenciador do comportamento

responsável relativo à Segurança da Informação. O Quadro 51 apresentado a seguir mostra a percepção dos gestores frente a essa relação de influência.

Quadro 51: Influência da variável moderadora Escolaridade no Comportamento

Influência Percebida	Frequência
Sim	11
Não	3

Fonte: O autor (2014)

De acordo com a percepção de 11 dos respondentes, a escolaridade atua como influenciadora do comportamento responsável do empregado frente à Segurança da Informação. Somente três gestores negaram essa relação de influência.

Em relação às categorias mais citadas dessa variável moderadora, podemos apresentar as seguintes: **Evidências de que funcionários com maior escolaridade têm comportamento mais responsável em relação à Segurança** e **Evidências de que funcionários com menor escolaridade têm comportamento mais responsável em relação à Segurança**. Com cinco observações e sete evidências conferidas, a categoria Evidências de que funcionários com maior escolaridade têm comportamento mais responsável em relação à Segurança diz respeito às afirmações de que colaboradores com um nível de escolaridade mais alto tendem a ter comportamentos mais adequados relativo à Segurança da Informação, o que pode ser visto no comentário do Gestor D, que inclusive cita exemplos verdadeiros para caracterizar esta relação:

> [...] A consciência sobre as principais ameaças depende muito da escolaridade. Tu vê pessoas com nível superior, que elas estudaram, elas sabem o impacto que ela pode ter, ela sabe por que ela não pode fazer determinadas coisas. O pessoal de mais baixa escolaridade, e aqui a gente tem desde pessoas de quinta série até pessoas com doutorado, então tu pega o pessoal do terminal, para eles é festa, eles não tem noção. Então, a escolaridade então faz muita diferença na consciência de como as ameaças se apresentam. A gente tem uma ferramenta de bloqueio de e-mail, mas a gente sempre está correndo atrás para bloquear novos tipos de spam com mensagens e tudo mais. O cara, por exemplo, aqui do administrativo, aí ele recebe uma mensagem assim: “Veja foto da sua mulher te traindo”. O cara sabe que é besteira e ele sabe que não é a mulher dele. É uma pagina php que vai baixar um worm ou alguma coisa assim. O cara do terminal acha que realmente é a mulher dele e clica, só que o nosso sistema bloqueia a internet e não deixa ele acessar o site. Mas, geralmente, quanto mais baixo o nível de escolaridade, mais suscetível essa pessoa é a ameaças digitais. E é esse o público que a maioria das ameaças tentam pegar. Pessoal que baixa porcaria, que acha que realmente é a foto da mulher dele que está ali. E, às vezes, o cara manda assim, ele recebeu, foi a muito tempo atrás, um cara da expedição de São Paulo, o cara recebeu esse e-mail, passou pelo nosso filtro, e o cara clicou. Nós bloqueamos a página, tem uma série de verificações que a gente faz, inclusive se tem algum código malicioso. Ele bloqueou, ele foi até nós e pediu: “Bah, libera a página para mim que tem foto da minha mulher me traindo”. Daí a gente falou: “Cara, não é. Não que a tua mulher não esteja te traindo. Até pode estar, mas esse e-mail não é sobre isso. É sacanagem mesmo”. [...]

Contrariando a ideia da categoria anterior, a categoria Evidências de que funcionários com menor escolaridade têm comportamento mais responsável em relação à Segurança obteve quatro citações e evidências descobertas. Apresentando relatos de que colaboradores com menor nível de escolaridade possuem um comportamento mais adequado relativo à Segurança da Informação, essa categoria pode ser ilustrada pelo comentário do Gestor I, dizendo que funcionários com maior escolaridade tendem a ter mais comportamentos de risco, o que não acontece com quem tem baixa escolaridade:

> [...] Eu acredito que sim, e eu acredito que sim em vários aspectos. Não é uma questão de dizer que, por exemplo, isso é uma coisa até engraçada, o cara que tem menos escolaridade vai causar mais problema, pode-se pensar num primeiro momento, mas eu acredito que é, justamente, o inverso. Quanto maior o poder aquisitivo e quanto maior o estudo, mais problemas você tem, porque quem não tem conhecimento ou tem pouco estudo, ele vai ter mais bloqueio em relação à tecnologia. Então assim, a não ser por mau uso, a tendência do cara é dizer assim: 'Não, isso aqui eu não conheço, eu vou chamar alguém que conheça para mexer'. Em compensação, você tem pessoas que já fizeram mestrado, doutorado, pós-doutorado, tem smartphones, tem tablets e tem um comportamento, às vezes, de risco. E eu não estou falando só da área de Segurança, às vezes de outras áreas, mas que, por exemplo, tem uma navegação, acessam extranet, no caso, ou acessam sistemas internos através de tablets aonde os arquivos temporários ficam gravados nesses tablets. E as pessoas não têm muito conhecimento que isso acontece. Então, eu acredito que tenha relação. Quanto maior o nível escolar, na minha visão, maior o risco associado pela exposição. [...]

Para o Gestor K, empregados que tem baixa escolaridade, por desconhecerem certas situações que podem ser vivenciadas, solicitam auxílio e não se expõem ao risco:

> [...] Eu acho que, muitas vezes, a pessoa que tem mais escolaridade tende a entender que ela conhece mais e vai um pouco mais além. A pessoa que não conhece, creio que depende muito. Eu não tenho esse dado de escolaridade, mas eu tenho casos em que pessoas que não tem escolaridade e que, por ter acontecido alguma coisa diferente na frente dela no computador, ela liga para o help desk. Então, eu tenho mais casos de pessoas que não tem muito treinamento, que só tem o 2º grau ou o cursinho profissionalizante, e elas entram mais em contato comigo pelo help desk para perguntar o que elas devem fazer. E outras pessoas que, talvez, tenham vivenciado mais, tenham computador desde criança ou ensino superior completo, elas tendem a arriscar mais. [...]

Abaixo, no Quadro 52, podem ser verificadas as categorias definidas na interpretação dos dados da variável estudada.

Quadro 52: Categorias da variável Escolaridade

Categorias	Frequência	Total de Evidências	Outras Evidências
Evidências de que funcionários com maior escolaridade têm comportamento mais responsável em relação à Segurança	5	7	E3 - [...] Eu percebo que sim, que isso influencia. Pessoas com baixo nível de escolaridade são mais manipuladas. Engenharia social. "Me empresta aqui a tua senha, escreve aqui." "Me dá o teu CPF". Isso ocorre e acontece. Ou phishing. Recebem um e-mail que diz: "Digite todo o seu cartão de crédito". Ingenuidade, isso é percebido. [...] E5 - [...] a pessoa que tem uma formação, uma pessoa que é mais instruída, uma pessoa com maior nível de instrução, a tendência é de que ela entenda mais os problemas que podem existir se uma informação não for bem protegida. [...] E7 - [...] Funcionários com maior escolaridade, normalmente, estão em cargos de maior responsabilidade e têm acesso a informações privilegiadas. Logo, eles tendem a ter melhor comportamento, mais adequados às suas funções. Já funcionários de nível baixo tendem a ter comportamentos inadequados, normalmente sem má intenção, mas que podem trazer vulnerabilidades e brechas de Segurança da Informação. [...]
Evidências de que funcionários com menor escolaridade têm comportamento mais responsável em relação à Segurança	4	4	E1 - [...] quem tem menor escolaridade costuma fazer uma atividade mais operacional e tem a regra mais ditada do que o cara que tem acesso. Normalmente, o cara que tem escolaridade maior tem acesso a um nível de informatização maior e então acaba utilizando e fazendo alguns vícios. [...] E3 - [...] A impressão que eu tenho é que, quanto menor for o nível de escolaridade, mais aderente as pessoas são, por incrível que pareça. Por questões de seguir as regras da empresa e tudo mais. [...]
Funcionários com maior escolaridade que têm comportamento menos responsável são exceções	1	1	E1 - [...] tem um outro viés na questão de escolaridade. São aquelas pessoas que se acham muito inteligentes. "Não vai acontecer". "Ninguém vai roubar minha senha". Mas também são exceções. [...]
Evidências de que funcionários com maior escolaridade têm comportamento menos responsável em relação à Segurança na área de TI	1	1	E1 - [...] as pessoas com maior escolaridade, mais esclarecidas, são as pessoas que estão vindo quentes da faculdade e do mercado e que querem também dar uma curva no sistema porque aprenderam a fazer isso. Então, eu vejo isso mais para o lado da área da TI. [...]

Fonte: O autor (2014)

O **Nível Hierárquico** é a última variável moderadora do comportamento responsável e aborda o nível hierárquico ou o cargo do colaborador como influenciador do comportamento adequado relativo à Segurança da Informação. O Quadro 53 mostra a relação percebida pelos gestores na variável.

Quadro 53: Influência da variável moderadora Nível Hierárquico no Comportamento

Influência Percebida	Frequência
Sim	11
Não	3

Fonte: O autor (2014)

Segundo 11 dos gestores entrevistados, o nível hierárquico ou o cargo do funcionário está relacionado com o comportamento adequado do empregado frente à Segurança da Informação, o que garante uma relação de influência. Apenas três respondentes não verificaram essa influência.

A categoria mais significativa na análise dessa variável foi **Evidências de que funcionários de nível hierárquico maior ou com cargos melhores têm comportamento menos responsável em relação à Segurança**. Apresentando relatos como forma de comprovação de que colaboradores de maior nível hierárquico ou com cargos mais altos tendem a manterem comportamentos inadequados relativo à Segurança da Informação, o caso real citado pelo Gestor D sugere esta realidade:

> [...] A gente teve em julho o encontro nacional de gerentes em São Paulo, todos os gerentes corporativos e os principais gerentes das unidades da empresa em São Paulo, reunidos para ver questões estratégicas e tudo mais. Isso foi no final de semana. No sábado à noite, em um jantar, um jantar de confraternização, e daí tem uísque e tal, era um jantar italiano. Eu tava com o meu Blackberry, daí eu estava na mesa, e tinha mais gente, eu resolvi dar uma olhada no Facebook e um dos gerentes botou um post no Facebook. Ele tirou uma foto com o Blackberry com todo mundo que estava na mesa dele e escreveu embaixo assim: 'Essa é e melhor parte da convenção, estamos todos bêbados'. Só que ele não se deu conta de que eles tem 70 pessoas, amigos que são da empresa, que não estavam lá, e eles não sabem que aquilo que estava falando era uma brincadeira. Então eles pensam: "Pô, a empresa não está bem financeiramente, todo mundo lá e a melhor parte da convenção é estar tudo mundo bêbado". Daí eu peguei, olhei a foto, vi mais ou menos a mesa onde ele estava pela foto e mostrei para o cara, e ele: "Ah, mas é só uma brincadeira". "Mas tu tens noção que essa tua brincadeira está postada para todo mundo ver, que as pessoas que não estão aqui não sabem que é uma brincadeira?". Então, é complicado. E já é um gerente corporativo, não é um peão. E não se deu conta do impacto. Talvez até quem esteja no nível operacional e não saiba lidar com computadores em geral, tenham comportamentos mais responsáveis. [...]

Conforme o ponto de vista do Gestor I, funcionários de nível hierárquicos maiores ou com cargos mais altos apresentam maior liberação de recursos tecnológicos ou de acesso e, por esse motivo, podem se comportar com menos responsabilidade sem serem notados:

> [...] Sim, com certeza. E, na verdade, aqui pode ser um contra-senso. Eventualmente, um executivo pode estar mais preocupado com determinados aspectos e menos com outros, em relação à Segurança. Por exemplo, ele pode estar mais preocupado em relação a uma certificação PCI, ou seja, ele vai fazer de tudo para implementar controles no armazenamento dos cartões de créditos, mas ele vai estar muito

> preocupado com a produtividade dele e vai querer que ele possa navegar liberado. Então, existem esses contra-sensos assim, mas estão vinculados, sim, aos cargos e ao nível hierárquico. Até porque, quando o nível é muito básico, operacional, às vezes, tático, você não tem muita inferência sobre o que você faz. Você, efetivamente, acaba entrando dentro de uma regra padrão para aquele nível e, dependendo, o funcionário vai querer, sei lá, acessar o bankline, que ele não poderia fazer dentro do horário comercial, ou Facebook, e ele vai tentar, de repente, burlar, por isso. E um gestor que tem o tempo liberado, eventualmente, ele vai fazer um acesso durante o horário e aquilo, por si só, de repente, não vai ser uma tentativa porque, para ele, na verdade, estaria liberado. [...]

A segunda categoria mais observada foi **Evidências de que funcionários de nível hierárquico maior ou com cargos melhores têm comportamento mais responsável em relação à Segurança**. Ela retrata os indícios encontrados de que colaboradores de nível hierárquico maior ou com cargos de nível mais alto tendem a manter um comportamento mais adequado frente à Segurança da Informação, o que pode ser resumido pela fala do Gestor N: "[...] Quanto maior o nível hierárquico, quanto mais alto for o cargo do funcionário, mais informações ele tem sobre Segurança. Assim, pessoas com cargos no nível estratégico tendem a ter comportamentos mais responsáveis em relação à Segurança da Informação [...]".

O Quadro 54 dispõe todas as categorias descobertas nesta variável, a frequência de citação e o número de evidências, além de outras caracterizações feitas pelos entrevistados.

Quadro 54: Categorias da variável Nível Hierárquico

Categorias	Frequência	Total de Evidências	Outras Evidências
Evidências de que funcionários de nível hierárquico maior ou com cargos melhores têm comportamento menos responsável em relação à Segurança	5	5	E1 - [...] Como já tinha dito, o cara que tem escolaridade maior também tem um cargo melhor. Logo, tem acesso a um nível de informatização maior e então acaba utilizando e fazendo alguns vícios. [...] E3 - [...] Aqui eu percebo assim. Digamos que tem aquela coisa, não só do familiar. Normalmente, os familiares estão numa hierarquia maior e eles conseguem acesso e solicitam acessos que não são de acordo com as atividades deles. [...]
Evidências de que funcionários de nível hierárquico maior ou com cargos melhores têm comportamento mais responsável em relação à Segurança	4	4	E2 - [...] Já o gerente, que tem dados sigilosos, ele não transfere esses dados toda a hora, por exemplo, não está na atividade dele, tem um impacto maior, mas até por ele ter um nível de responsabilidade maior com o grau hierárquico, ele precisa se preocupar mais com isso. [...]
O nível hierárquico ou o cargo não são determinantes no comportamento responsável em relação à Segurança	2	2	E1 - [...] Dependendo da cultura da empresa, se existe uma cultura da empresa ou de Segurança, que não tem regras muito claras de Segurança ou nem tem política de Segurança, pensando numa situação dessas, também não tem valores muito bem definidos e não tem uma cultura forte, a pessoa que está num nível hierárquico maior também pode sentir que tem mais liberdade e pode fazer o que quiser. Isso depende muito da cultura da empresa e do meio onde a pessoa está [...] E2 - [...] na realidade, não é pelo cargo, mas é por tudo aquilo que agrega o sujeito a estar numa linha maior na empresa, numa hierarquia maior na empresa. É o conjunto, não é exclusivamente o cargo. É a experiência, é a bagagem, é a instrução, é o coeficiente de 'cagaço', enfim. [...]

Fonte: O autor (2014)

Com a finalização da interpretação individual de todas as variáveis pertencentes à dimensão Comportamento Responsável Relativo à Segurança da Informação, faremos uma análise geral com base no Quadro 55, disponível a seguir.

Quadro 55: Percepções do Comportamento Responsável Relativo à Segurança da Informação no sentido de Proteger Contra Vulnerabilidades a Ameaças Internas de Segurança da Informação

DIMENSÕES	VARIÁVEIS	PERCEPÇÕES
Comportamento Responsável Relativo à Segurança da Informação	Disseminação do Comportamento	Na Política
	Treinamento, Capacitação e Conscientização	Percebida como influente
	Política de Segurança da Informação como Mecanismo de Proteção	Atender somente a Política
	Juízo de Comportamento Relacionado à Política de Segurança da Informação	Nenhuma das situações descritas
	Seriedade da Violação de Regras e Normas	Percebida como influente*
	Prejudicialidade da Violação de Regras e Normas	Percebida como não influente
	Legitimidade da Violação de Regras e Normas	Percebida como não influente
Moderadores do Comportamento Responsável	Gênero	Percebida como não influente*
	Lealdade à Empresa	Percebida como influente
	Escolaridade	Percebida como influente
	Nível Hierárquico	Percebida como influente

* Poucos indícios de influência percebida ou não percebida

Fonte: O autor (2014)

A relação de influência do comportamento responsável relativo à Segurança da Informação na proteção contra vulnerabilidades a ameaças internas de Segurança da Informação foi considerada inconclusiva, pois houve o mesmo número de influências percebidas e não percebidas pelos gestores investigados. O que se pode afirmar é que a Política de Segurança da Informação é o principal elemento de proteção utilizado pelas empresas, tanto no sentido de apresentar e difundir o comportamento responsável como no sentido de contribuir para a proteção contra vulnerabilidades a ameaças internas de Segurança da Informação.

Quanto ao juízo de comportamento relativo à Política de Segurança, nenhuma das duas situações propostas no roteiro de entrevistas foi considerada válida a ponto de evitar vulnerabilidades a ameaças internas de Segurança, ou seja, fazer somente o que é permitido na Política de Segurança ou considerar corretas situações fora da Política de Segurança concretizadas não é o comportamento esperado ou desejável pela organização, pois sempre se espera algo mais do funcionário no sentido de ter atitudes condizentes com os princípios ou valores da empresa, além de seguir o Código de Ética da instituição. Entretanto, em casos consolidados onde não há especificação na Política de Segurança da Informação, a avaliação

individual do fato é a alternativa mais empregada, sendo que, após a resolução e a ponderação do caso, este deve ser incluído em uma próxima revisão ou atualização da Política de Segurança. Em relação à intensidade das percepções das variáveis descritas do Comportamento Responsável Relativo à Segurança da Informação, somente uma obteve poucos indícios de influência percebida, que foi na variável Seriedade da Violação de Regras e Normas. Todas as outras variáveis tiveram indícios mais fortes, tanto positiva quanto negativamente.

Em relação aos moderadores do Comportamento Responsável, três variáveis tiveram a influência percebida, com exceção da variável Gênero. No entanto, na mesma variável Gênero, houve poucos indícios de que a relação de influência não foi percebida, já que a diferença entre as respostas negativas e positivas foi relativamente baixa (duas respostas). Nas outras variáveis moderadoras, os indícios foram considerados fortes.

Adiante, seguiremos com a etapa referente aos fatores desencadeadores do comportamento responsável dos funcionários relacionado à Segurança da Informação.

4.5 FATORES DESENCADEADORES DO COMPORTAMENTO RESPONSÁVEL RELATIVO À SEGURANÇA DA INFORMAÇÃO

Como forma de abranger o quarto e último objetivo específico desta pesquisa, a identificação dos fatores desencadeadores do Comportamento Responsável dos colaboradores Relativo à Segurança da Informação no sentido de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação compreende esta seção. Na realização desta etapa da pesquisa, feita a partir da consolidação das categorias descobertas em cada variável das dimensões Contexto Organizacional e Contexto de Tecnologia e Segurança da Informação, foi possível verificar os fatores que podem contribuir efetivamente para o comportamento considerado adequado dos empregados frente à Segurança da Informação, conforme a percepção dos gestores entrevistados. Em cada uma das variáveis pesquisadas, foi delimitado um fator desencadeador do comportamento responsável relacionado à Segurança da Informação, a partir da síntese conjunta das categorias que obtiveram maior frequência de observações na sua respectiva variável. No Quadro 56, serão apresentados os fatores desencadeadores do comportamento responsável como forma de prover boas práticas a serem desempenhadas pelas organizações e que favorecem a proteção contra vulnerabilidades a ameaças internas de Segurança da Informação.

Quadro 56: Fatores Desencadeadores do Comportamento Responsável Relativo à Segurança da Informação

DIMENSÕES	VARIÁVEIS	FATORES DESENCADEADORES DO COMPORTAMENTO RESPONSÁVEL
Contexto de Tecnologia e Segurança da Informação	Conhecimento e Habilidades	**Proporcionar familiaridade dos funcionários com Segurança da Informação**
	Experiência e Conhecimentos Gerais em TI	**Fornecer conscientização e proporcionar familiaridade dos funcionários com Tecnologia da Informação**
	Conhecimento da Política de Segurança da Informação	**Melhorar a divulgação da Política de Segurança da Informação**
	Severidade da Política de Segurança da Informação	**Ter uma Política de Segurança da Informação orientativa e conscientizadora, porém com aplicação prática da punição quando necessário**
	Mecanismos de Controle como Inibidores do Desempenho e da Criatividade	**Ter Políticas e controles de Segurança da Informação diferenciados para cada ambiente/setor específico, de acordo com a necessidade do negócio/atividade e da tecnologia a ser utilizada**
	Mecanismos de Controle da Violação de Regras e Normas	**Ter níveis diferenciados de sanções, desde uma orientação até uma demissão por justa causa, aplicada de acordo com cada caso**
	Punição como Inibidor da Reincidência de Eventos de Segurança da Informação	**Aplicar punições na prática, quando necessário, como exemplo para orientar e conscientizar os funcionários**
	Monitoramento	**Manter monitoramento consciente e constante para verificação quando necessário**
	Monitoramento como Inibidor de Eventos de Segurança da Informação	**Utilizar o monitoramento consciente para orientar o comportamento**
Contexto Organizacional	Clima Organizacional	**Proporcionar um ambiente organizacional que favoreça o clima percebido pelos colaboradores em geral**
	Fluxo de Trabalho de Segurança da Informação	**Aplicar somente regras de Segurança necessárias, conforme a avaliação do risco, para não interferir no dinamismo das atividades de negócio**
	Cultura Organizacional	**Manter uma cultura organizacional com valores bem definidos e voltada para a Segurança da Informação**
	Relação entre Funcionários e seus Superiores	**Cultivar boas relações entre funcionários e superiores**
	Condições de Trabalho	**Proporcionar condições de trabalho adequadas**
	Diferenças entre Ambientes Organizacionais	**Aplicar a Política de Segurança da Informação independentemente do ambiente organizacional**
	Comportamento dos Pares	**Proporcionar um ambiente em que todos tenham consciência da necessidade da Segurança da Informação**
	Satisfação com o Trabalho	**Promover a satisfação dos funcionários**

Fonte: O autor (2014)

O primeiro fator considerado desencadeador é **Proporcionar familiaridade dos funcionários com Segurança da Informação**, localizado na variável Conhecimento e Habilidades, e aborda a familiaridade que os colaboradores devem ter para garantir um comportamento responsável frente à Segurança da Informação. Para isso, a empresa precisa proporcionar essa familiaridade para nivelar todos os empregados na capacidade de proteger

contra vulnerabilidades a ameaças internas de Segurança da Informação, o que pode ser alcançado por meio de treinamentos e programas de capacitação ou conscientização.

O segundo fator desencadeador do comportamento responsável é **Fornecer conscientização e proporcionar familiaridade dos funcionários com Tecnologia da Informação**, encontrado na variável Experiência e Conhecimentos Gerais em TI, e diz respeito ao fornecimento de conscientização e de familiaridade aos empregados com Tecnologia da Informação. Nesse sentido, a empresa também necessita equiparar o nível de conscientização e familiaridade dos colaboradores, a fim de manter uma gestão de Segurança da Informação relativamente segura. Treinamentos e programas de capacitação e conscientização também são os melhores caminhos a serem seguidos.

Quanto ao terceiro fator descoberto, temos **Melhorar a divulgação da Política de Segurança da Informação**, relativo à variável Conhecimento da Política de Segurança da Informação, e retrata a necessidade de melhorar a disseminação da Política de Segurança da Informação para fornecer o conhecimento necessário aos funcionários, contribuindo para um comportamento mais responsável. Para melhorar a divulgação da Política de Segurança, a empresa deve utilizar diferentes meios que possam alcançar todos ambientes e níveis da organização de maneira diferenciada.

Como quarto fator verificado, encontrado na variável Severidade da Política de Segurança da Informação, observou-se **Ter uma Política de Segurança da Informação orientativa e conscientizadora, porém com aplicação prática da punição quando necessário**. Isto significa que a Política de Segurança deve ter uma abordagem orientativa e conscientizadora no sentido de fornecer subsídios para o comportamento responsável dos colaboradores. No entanto, as punições também devem estar contempladas nesta Política e a aplicação prática da punição é de extrema importância, conforme a análise do caso, que fica a critério de cada organização.

O quinto fator desencadeador foi observado na variável Mecanismos de Controle como Inibidores do Desempenho e da Criatividade e é **Ter Políticas e controles de Segurança da Informação diferenciados para cada ambiente/setor específico, de acordo com a necessidade do negócio/atividade e da tecnologia a ser utilizada**. Isto significa que as Políticas de Segurança e os mecanismos de controle devem existir, mas com elementos específicos para cada ambiente ou setor diferente, conforme a necessidade do negócio ou da atividade desempenhada no ambiente/setor e da tecnologia a ser empregada.

Quanto ao sexto fator identificado, foi observado **Ter níveis diferenciados de sanções, desde uma orientação até uma demissão por justa causa, aplicada de acordo**

com cada caso, reconhecido na variável Mecanismos de Controle da Violação de Regras e Normas. Conforme cada violação ou incidente de Segurança da Informação, intencional ou não intencional, de baixo ou alto risco envolvido, reincidência ou não, deve ter punições adequadas a cada situação. Uma orientação verbal pode reeducar um colaborador que teve uma falta de atenção momentânea e uma demissão por justa causa pode servir como exemplo para todos os empregados em caso de uma reincidência de alto risco ou de uma violação intencional.

Em relação ao sétimo fator que favorece o comportamento adequado dos empregados frente à Segurança da Informação, temos **Aplicar punições na prática, quando necessário, como exemplo para orientar e conscientizar os funcionários**, localizado na análise da variável Punição como Inibidor da Reincidência de Eventos de Segurança da Informação. Esse fator reitera a necessidade da aplicação prática das punições previstas na Política de Segurança da Informação em casos onde a organização julgue adequada, para servir de modelo na orientação e na conscientização dos colaboradores.

Relativo ao oitavo fator descoberto, observado na variável Monitoramento, temos **Manter monitoramento consciente e constante para verificação quando necessário**. A manutenção de um monitoramento constante previamente avisado aos colaboradores incita um maior cuidado no trato com Segurança da Informação, proporcionando comportamentos mais responsáveis. Não existe a necessidade da aplicação de um monitoramento em tempo real, com verificação e análise no momento do acontecimento, pois diversos softwares fazem esse papel em situações críticas, porém os registros do monitoramento servem para identificação de possíveis incidentes de Segurança.

O nono fator que promove o comportamento responsável dos empregados é **Utilizar o monitoramento consciente para orientar o comportamento**, da variável Monitoramento como Inibidor de Eventos de Segurança da Informação. O uso do monitoramento com o consentimento dos funcionários serve, implicitamente, para promover o comportamento responsável visando evitar vulnerabilidades a ameaças internas de Segurança da Informação.

Quanto ao décimo fator desencadeador, foi identificado **Proporcionar um ambiente organizacional que favoreça o clima percebido pelos colaboradores em geral**, junto à variável Clima Organizacional. Isto significa que o clima organizacional do ambiente em que o funcionário está inserido deve ser favorável, o que proporciona bem estar aos empregados em geral e favorece o comportamento responsável.

O décimo primeiro fator facilitador do comportamento responsável encontrado foi **Aplicar somente regras de Segurança necessárias, conforme a avaliação do risco, para**

não interferir no dinamismo das atividades de negócio, visto na variável Fluxo de Trabalho de Segurança da Informação. Tratando da aplicação de regras e normas de Segurança da Informação apenas quando realmente houver necessidade e segundo a avaliação de risco realizada pela empresa, ele visa não intervir na dinâmica dos processos de negócio da organização e não sobrecarregar o fluxo de trabalho relativo aos procedimentos de Segurança da Informação.

Relacionado ao décimo segundo fator desencadeador determinado, referente à variável Cultura Organizacional, temos **Manter uma cultura organizacional com valores bem definidos e voltada para a Segurança da Informação**. Uma cultura organizacional com princípios e valores marcantes difundidos entre os funcionários e que valorizem a Segurança da Informação consegue fornecer bons subsídios para um comportamento relativamente mais seguro.

Descoberto na variável Relação entre Funcionários e seus Superiores, o décimo terceiro fator facilitador do comportamento responsável é **Cultivar boas relações entre funcionários e superiores**. Isto proporciona melhores condições para incentivar o comportamento adequado, fazendo do gestor um exemplo a ser seguido pelos membros de sua equipe.

Na variável Condições de Trabalho, foi observado o décimo quarto fator que pode originar o comportamento responsável, **Proporcionar condições de trabalho adequadas**. As condições de trabalho oferecidas pela organização devem ser condignas com a natureza da atividade do negócio para não afetar no desempenho comportamental do colaborador.

O décimo quinto fator que pode determinar o comportamento responsável dos funcionários é **Aplicar a Política de Segurança da Informação independentemente do ambiente organizacional**, verificado na variável Diferenças entre Ambientes Organizacionais. A aplicação prática da Política de Segurança da Informação em qualquer tipo de ambiente, seja ele considerado cooperativo, competitivo ou misto, impede desvios de conduta que podem ser facilitados em certos ambientes.

Relacionado ao décimo sexto fator identificado, componente da variável Comportamento dos Pares, temos **Proporcionar um ambiente em que todos tenham consciência da necessidade da Segurança da Informação**. Como todo o comportamento dos colaboradores é influenciado pelos seus colegas mais próximos, a manutenção de um ambiente que proporcione a percepção da necessidade intrínseca de maneiras para garantir a Segurança da Informação terá impacto na grande maioria dos funcionários.

O último fator desencadeador do comportamento responsável identificado foi **Promover a satisfação dos funcionários**, relacionado à variável Satisfação com o Trabalho. Ao promover o bem estar e a felicidade dos colaboradores, seja por fornecer os recursos desejados, pela forma de como executar sua atividade ou outro aspecto específico, o comportamento responsável dos funcionários também será favorecido.

Com a observação destes 17 fatores desencadeadores do comportamento responsável dos colaboradores relativo à Segurança da Informação, é possível canalizar os esforços para garantir um ambiente relativamente seguro na intenção de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação.

Com o fim da explanação sobre os fatores desencadeadores do comportamento responsável relativo à Segurança da Informação, conclui-se a etapa de resultados da pesquisa desenvolvida e as considerações finais são destaque no capítulo a seguir.

5 CONSIDERAÇÕES FINAIS

Neste último capítulo são realizadas as considerações finais a respeito da pesquisa desenvolvida, que tinha como objetivo principal identificar a relação de influência do contexto no comportamento responsável relativo à Segurança da Informação. As conclusões dos resultados encontrados, assim como as contribuições para o campo de pesquisa, as contribuições gerenciais para as organizações, os limites do estudo e as sugestões de pesquisas futuras serão apresentados a seguir.

5.1 CONCLUSÕES

Esta pesquisa teve como objetivo principal identificar a relação de influência dos contextos organizacional e de tecnologia e Segurança da Informação no comportamento responsável dos colaboradores em relação à Segurança da Informação visando evitar vulnerabilidades a ameaças internas de Segurança da Informação, segundo a percepção dos gestores entrevistados. A partir do modelo conceitual desenvolvido conforme o referencial pesquisado e da análise de conteúdo categorial das entrevistas realizadas, foi possível verificar as relações de influência percebidas em cada variável dos contextos pesquisados no comportamento responsável dos funcionários, assim como as práticas ou os esforços empregados para a manutenção de toda a gestão da Segurança da Informação das organizações pesquisadas.

Conforme a interpretação realizada de acordo com a percepção dos respondentes, pode-se afirmar que, tanto o contexto organizacional quanto o contexto de tecnologia e Segurança da Informação exercem influência no comportamento responsável dos funcionários frente à Segurança da Informação no sentido de proteger contra vulnerabilidades a ameaças internas de Segurança da Informação.

Das variáveis pertencentes à dimensão Contexto Organizacional, todas obtiveram a relação de influência percebida no comportamento confirmada pelos gestores, sem nenhuma exceção. A confirmação destes achados encontra suporte na pesquisa realizada por Chan, Woon e Kankanhalli (2005) relativos ao clima organizacional e a influência no comportamento individual relacionado à Segurança da Informação, assim como no estudo feito por Albrechtsen (2007) sobre o fluxo de trabalho empregado em Segurança da Informação, nos trabalhos de Chang e Lin (2007) e Van Niekerk e Von Solms (2010) sobre cultura organizacional no ambiente de Segurança da Informação, na publicação de Vroom e

Von Solms (2004) sobre a relação entre funcionários e seus supervisores e condições de trabalho afetando a Segurança da Informação e no artigo de Herath e Rao (2009a) sobre o comportamento dos pares em um ambiente de Segurança.

Na dimensão Contexto de Tecnologia e Segurança da Informação, a maior parte das variáveis resultaram na ratificação da relação de influência percebida no comportamento, exceto nas variáveis Conhecimento e Habilidades e Mecanismos de Controle da Violação de Regras e Normas, que não tiveram influência percebida pelos gestores (a variável Conhecimento e Habilidades ainda obteve poucos indícios da influência não percebida), e Mecanismos de Controle como Inibidores do Desempenho e da Criatividade, que foi considerada inconclusiva, visto que não houve definição do total de entrevistados quanto à relação de influência percebida ou não percebida. É importante ressaltar que tanto a variável Severidade da Política de Segurança da Informação e a variável Punição como Inibidor da Reincidência de Eventos de Segurança da Informação foram consideradas influentes no comportamento responsável de Segurança da Informação, o que não havia sido confirmado na pesquisa sobre este mesmo assunto publicada por Herath e Rao (2009a). Já as variáveis de monitoramento foram confirmadas como influentes no comportamento responsável dos colaboradores, como apresentado no artigo desenvolvido por D'Arcy, Hovav e Galletta (2008).

No entanto, a relação de influência do Comportamento Responsável Relativo à Segurança da Informação visando Proteger Contra Vulnerabilidades a Ameaças Internas de Segurança da Informação foi considerada inconclusiva, visto que o número de influências percebidas foi o mesmo de influências não percebidas. Treinamento, Capacitação e Conscientização e Seriedade da Violação de Regras e Normas, variáveis que foram suportadas por Lee, Lee e Yoo (2004), também obtiveram influência percebida (sendo que a última obteve poucos indícios de relação de influência confirmada). Somente as variáveis Prejudicialidade da Violação de Regras e Normas e Legitimidade da Violação de Regras e Normas não tiveram influência percebida pelos respondentes. Como a abordagem nesta dimensão foi diferente da forma realizada nas duas dimensões anteriores, as maneiras descritas nestas variáveis foram específicas. Assim, foi possível afirmar que a Política de Segurança da Informação é a base fundamental para garantir a proteção da Segurança da Informação das organizações, usada na intenção de fornecer e divulgar o comportamento responsável, além de colaborar na proteção contra vulnerabilidades a ameaças internas de Segurança da Informação. Em relação à variável Juízo de Comportamento Relacionado à Política de Segurança da Informação, foi possível verificar que as empresas sempre esperam

mais do colaborador no sentido de ter sua conduta baseada nos princípios e valores da organização, assim como seguir o Código de Ética da instituição. É importante salientar que em situações concretizadas onde não houver especificação na Política de Segurança da Informação, a análise individual do caso é a opção frequentemente escolhida e que, posteriormente, será utilizada para atualizar a Política de Segurança da Informação em momento oportuno.

Quanto aos moderadores do Comportamento Responsável, pode-se afirmar que a maioria das variáveis descritas fazem parte da influência moderadora no comportamento responsável relacionado com Segurança da Informação. A única exceção foi da variável Gênero, que obteve poucos indícios de influência não percebida, porém foi sugerida por diversas outras pesquisas anteriores como influente que consideravam o gênero feminino como o mais responsável relativo a ações de Segurança da Informação.

Assim, o estudo mostra que manter os ambientes seguros é tarefa de toda a organização, não podendo ser entendida apenas como uma responsabilidade do funcionário: a organização deve, ao mesmo tempo, indicar claramente qual é o comportamento desejado e criar mecanismos para conduzir os usuários a se comportarem da forma indicada. A ação mais comum é indicar via Política de Segurança da Informação o que não é permitido, deixando para que cada usuário conclua por si mesmo qual é o comportamento esperado. Nesse sentido, a identificação dos fatores desencadeadores do comportamento responsável relativo à Segurança da Informação fornece subsídios interessantes para uma gestão de Segurança da Informação mais segura.

5.2 CONTRIBUIÇÕES

Diversas contribuições podem ser relatadas a partir desta pesquisa, trazendo tanto implicações práticas e gerenciais quanto implicações para a área de conhecimento de Gestão da Informação. Por se tratar de um estudo sobre aspectos humanos e comportamentais relacionado com Segurança da Informação considerando uma abordagem diferente da maioria das pesquisas científicas que são baseadas em aspectos técnicos, este trabalho conseguiu prover resultados significativos com fortes indícios da relação de influência em diversos fatores do contexto organizacional e do contexto de Tecnologia e Segurança da Informação no comportamento responsável dos colaboradores, o que contribui plenamente para o campo de pesquisa da área em questão.

Também como contribuição para a área acadêmica podemos considerar a validação das dimensões abordadas no trabalho, o que inclui o modelo conceitual utilizado como embasamento para toda a pesquisa. Apesar da validação do modelo conceitual não estar prevista como um dos objetivos deste estudo, diversas variáveis pesquisadas e inclusas neste modelo foram confirmadas no resultado da análise, o que também caracteriza uma implicação para a área de estudo. O roteiro de entrevistas elaborado também traz contribuições para o campo de Gestão da Informação, pois pode ser aplicado em diferentes realidades ou cenários para posterior comparação. A complexidade das variáveis estudadas no âmbito da Segurança da Informação demonstra uma boa fundamentação teórica e uma ampla aplicabilidade no campo de atuação, inclusive com a identificação de outros fatores humanos e comportamentais que não foram abordados em pesquisas anteriores.

Os fatores desencadeadores que antecedem e que podem determinar o comportamento responsável dos funcionários frente à Segurança da Informação também são contribuições relevantes tanto para a área de pesquisa quanto para a área empresarial, visto que fornecem insights para pesquisas confirmatórias futuras e também fornecem para as organizações medidas efetivas para a realização de boas práticas que contribuem para a gestão da Segurança da Informação. Ainda nesta questão, uma das principais contribuições que se pode observar é a percepção gerencial prática, vista pelos gestores de TI, da realidade empresarial de Segurança da Informação de organizações do cenário nacional, destacando novos pontos importantes a serem estudados e confirmando outros fatores já abordados.

A preocupação com os fatores humanos e comportamentais também deve ser considerado na Segurança da Informação das empresas e traz implicações gerenciais importantes. O conhecimento proporcionado pelo estudo em questão aponta para uma visão holística que contemple aspectos comportamentais e técnicos de Segurança da Informação, pois somente assim uma Política de Segurança da Informação pode se tornar um importante instrumento na proteção contra vulnerabilidades a ameaças internas de Segurança da Informação.

5.3 LIMITES DA PESQUISA

Como toda pesquisa científica, certos limites foram observados na realização deste estudo. A pesquisa contou com somente quatorze gestores entrevistados, pois houve indisponibilidade de algumas empresas contatadas. Logo, o número de entrevistados diminuiu frente às opções iniciais e, com a indisponibilidade de certas organizações, a seleção dos

respondentes teve que ser por conveniência das empresas que tiveram a pretensão de participar da entrevista.

Pelo fato de que apenas um pequeno número das empresas investigadas disponibilizou a Política de Segurança da Informação ou qualquer outro documento relacionado à Segurança da Informação, não foi possível fazer uma triangulação dos dados obtidos a partir das entrevistas consolidadas. Logo, não houve um cotejamento dos dados analisados, o que pode ser considerado um limite para a pesquisa. Mais um limitante deste estudo pode ser o uso do modelo conceitual somente como forma de norteamento da pesquisa, já que, apesar de diversas relações de influências percebidas terem sido encontradas, a validação do modelo não estava entre os objetivos deste trabalho.

Outro limite estabelecido, clássico em estudos qualitativos, é a impossibilidade de generalizar os resultados. Entretanto, esses resultados servem como possibilidade futura de estudo a partir de um dos temas específicos desta pesquisa. Mais um limitante do trabalho é a amplitude da pesquisa, que tratou apenas do contexto nacional, mais um fato que impede a generalização dos resultados obtidos no estudo e que certamente traria diferentes resultados se fosse feita em países com culturas diferentes.

5.4 SUGESTÕES DE PESQUISAS FUTURAS

Como sugestão para pesquisas futuras surgem diversas possibilidades. É possível testar estatisticamente o modelo conceitual utilizado no estudo a partir de uma abordagem quantitativa, o que pode fornecer uma validação devidamente comprovada. Também existe a possibilidade da realização de uma pesquisa survey confirmatória, para confirmar as relações de influência percebida pelos gestores entrevistados.

Outras oportunidades de estudo aparecem ao investigar cada contexto visto nesta pesquisa separadamente, a fim de poder generalizar os resultados pela estatística. Em trabalhos quantitativos também é possível verificar especificamente quanto cada variável estudada influencia no comportamento responsável dos colaboradores. Para melhor qualificação do novo trabalho, no caso da realização de um estudo quantitativo baseado nesta pesquisa, será necessário desmembrar o trabalho por contexto ou por grupo de determinadas variáveis.

Os fatores desencadeadores do comportamento responsável também servem de inspiração para outras pesquisas, pois agregam valor tanto para a teoria quanto para as implicações práticas. Estudos de caso individuais ou múltiplos também podem ser

desenvolvidos a partir da ideia deste trabalho. Como última sugestão, estudos específicos com esta pesquisa em outros países podem mostrar aspectos comportamentais completamente diferentes, já que o Brasil apresenta uma cultura peculiar relativa à Segurança da Informação, o que, provavelmente, trará resultados diferentes destes aqui encontrados.

REFERÊNCIAS

AAKER, D.; KUMAR, V.; DAY, G. **Pesquisa de marketing.** São Paulo: Atlas, 2004.

ABDELFATTAH, B.; MAHMOOD, M. A.; LUCIANO, E. M.; GEMOETS, L. Employee computer misuse: An empirical research. **40th Decision Sciences Conference**, New Orleans, 2009.

ABNT. **NBR ISO/IEC 17799: Tecnologia da informação - Código de prática para a gestão de segurança da informação**. Rio de Janeiro, 2001.

ABNT. **NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação**. Rio de Janeiro, 2005.

ABNT. **NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - requisitos**. Rio de Janeiro, 2006.

ACQUISTI, A.; GROSSKLAGS, J. Privacy and rationality in individual decision making: Economics of information security. **IEE Security and Privacy**, v.3, n.1, p.26-33, 2005.

ALAGAR, V. S. A human approach to the technological challenges in data security. **Computers & Security**, v.5, p.328-335, 1986.

ALBERTIN, A. L.; PINOCHET, L. H. C. **Política de segurança de informações: Uma visão organizacional para a sua formulação**. São Paulo: Elsevier, 2010.

ALBRECHTSEN, E. A qualitative study of users' view in information security. **Computers & Security**, v.26, n.4, p. 276-289, 2007.

ALBRECHTSEN, E.; HOVDEN, J. The information security digital divide between information security managers and users. **Computers & Management**, v.28, p.476-490, 2009.

ALDER, G. S.; NOEL, T. W.; AMBROSE, M. L. Clarifying the effects of internet monitoring on job attitudes: The mediating role of employee trust. **Information & Management**, v.43, p.894-903, 2006.

ANDERSON, C. L.; AGARWAL, R. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. **MIS Quarterly**, v.34, n.3, p.613-643, 2010.

ASHENDEN, D. Information security management: A human challenge? **Information Security Technical Report**, v.13, p.195-201, 2008.

BANG, Y.; LEE, D.; BAE, Y.; AHN, J. Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. **International Journal of Information Management**, p.1-10, 2012.

BARDIN, L. Análise de conteúdo. Lisboa: Edições 70, 2011.

BAUER, M. W.; GASKELL, G. **Pesquisa qualitativa com texto, imagem e som**: um manual prático. 3. ed. Petrópolis: Vozes, 2004.

BEAL, A. **Segurança da informação: Princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BOSS, S. R.; KIRSCH, L. J.; ANGERMEIER, I.; SHINGLER, R. A.; BOSS, R. W. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. **European Journal of Information Systems**, v.18, p.151-164, 2009.

BOZIONELOS, N. Computer anxiety: Relationship with computer experience and prevalence. **Computers in Human Behavior**, v.17, p.213-224, 2001.

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, 2010.

CARTWRIGHT, S.; HOLMES, N. The meaning of work: the challenge of regaining employee engagement and reducing cynicism. **Human Resource Management Review**, v.16, p.199-208, 2006.

CHAN, M., WOON, I. e KANKANHALLI, A. Perceptions of information security at the workplace: Linking information security climate to compliant behavior. **Journal of Information Privacy and Security**, v.1, n.3, p.18-41, 2005.

CHANG, S. E.; HO, C. B. Organizational factors to the effectiveness of implementing information security management. **Industrial Management & Data Systems**, v.106, n.3, p.345-361, 2006.

CHANG, S. E.; LIN, C. Exploring organizational culture for information security management. **Industrial Management & Data Systems**, v.107, n.3, p.438-458, 2007.

CHO, V. A study of the roles of trusts and risks in information-oriented online legal services using an integrated model. **Information & Management**, v.43, n.4, p.502-520, 2006.

CHODEN, K.; MAHMOOD, M. A.; MUKHOPADHYAY, S.; LUCIANO, E. M. Organizational preparedness for information security breaches: An empirical investigation. **40th Decision Sciences Conference**, New Orleans, 2009.

CHOO, C. W. **A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões**. São Paulo: Senac São Paulo, 2006.

COOPER, D.; SCHINDLER, P. **Métodos de pesquisa em administração.** Porto Alegre: Bookman, 2003.

CORONADO, A. S.; MAHMOOD, M. A.; PAHNILA, S.; LUCIANO, E. M. Measuring effectiveness of information systems security: An empirical research. **Proceedings of the Fifteenth Americas Conference on Information Systems**, San Francisco, EUA, 2009.

D'ARCY, J.; HOVAV, A. Does one size fit all? Examining the differential effects of IS security countermeasures. **Journal of Business Ethics**, v.89, p.59-71, 2009.

D'ARCY, J.; HOVAV, A.; GALLETTA, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. **Information Systems Research**, Articles in Advance, p. 1-20, 2008.

DA VEIGA, A.; ELOFF, J. H. P. A framework and assessment instrument for information security culture. **Computers & Security**, v.29, n.2, p.196-207, 2010.

DHILLON, G.; BACKHOUSE, J. Current directions in IS security research: Towards socio-organizational perspectives. **Information Systems Journal**, v.11, p.127-153, 2001.

DOURISH, P.; ANDERSON, K. Collective information practice: Exploring privacy and security as social and cultural phenomena. **Human-Computer Interaction**, v.21, p.319-342, 2006.

DULEBOHN, J. H.; MOLLOY, J. C.; PICHLER, S. M.; MURRAY, B. Employee benefits: Literature review and emerging issues. **Human Resource Management Review**, v.19, p.86-103, 2009.

DUTTA, A.; ROY, R. Dynamics of organizational information security. **System Dynamics Review**, v.24, n.3, p.349-375, 2008.

EY GLOBAL. EY's global information security survey 2013. **Ernst & Young Global Limited**, 2013.

FLICK, U. **Introdução à pesquisa qualitativa**. Porto Alegre: Bookman, 2004.

FONTES, E. **Segurança da informação: O usuário faz a diferença**. Rio de Janeiro: Saraiva, 2006.

GIBBS, G. **Análise de dados qualitativos**. Porto Alegre: Bookman, 2009.

GILBERT, F. Breach of system security and theft of data: Legal aspects and preventive measures. **Computers & Security**, v.11, n.6, p.508-517, 1992.

GOODHUE, D. L.; STRAUB, D. W. Security concerns of system users: A study of perceptions of the adequacy of security. **Information & Management**, v.20, n.1, p.13-27, 1991.

GUPTA, M.; REES, J.; CHATURVEDI, A.; CHI, J. Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. **Decision Support Systems**, v.41, p.592-603, 2006.

HAIR JR., J. F.; BABIN, B.; MONEY, A. H.; SAMOUEL, P. Fundamentos de métodos de pesquisa em administração. Porto Alegre: Bookman, 2005.

HANCOCK, B. CSI/FBI survey: Cyberattacks on the rise. **Computers & Security**, v.18, n.3, p.188-189, 1999.

HANSSON, S. O. A note on social engineering and the public perception of technology. **Technology in Society**, v.28, p.389-392, 2006.

HENDERSON, J. C.; VENKATRAMAN, N. Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal, v.32, n.1, p.4-16, 1993.

HERATH, T.; RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. **Decision Support Systems**, v.47, p.154-165, 2009a.

HERATH, T.; RAO, H. R. Protection motivation and deterrence: A framework for security policy compliance in organizations. **European Journal of Information Systems**, v.18, p.106-125, 2009b.

HOFSTEDE, G.; HOFSTEDE, G. J.; MINKOV, M. **Cultures and organizations: Software of the mind - Intercultural cooperation and its importance for survival**. London: McGraw-Hill, 2010.

HU, Q.; DINEV, T. Is spyware an internet nuisance or public menace? **Communications of The ACM**, v.48, n.8, p.61-66, 2005.

HU, Q.; HART, P.; COOKE, D. The role of external and internal influences on information systems security - A neo-institutional perspective. **Journal of Strategic Information Systems**, v.16, p.153-172, 2007.

HUANG, C. D.; HU, Q.; BEHARA, R. S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. **International Journal of Production Economics**, v.114, n.2, p.793-804, 2008.

HUI, K.; TEO, H. H.; LEE, S. T. The value of privacy assurance: An exploratory field experiment. **MIS Quarterly**, v.31, n.1, p.19-33, 2007.

HUMAIDI, N.; BALAKRISHNAN, V. Leadership Styles and Information Security Compliance Behavior: The mediator effect of information security awareness. **International Journal of Information and Education Technology**, Articles in Advance, v.5, n.4, p.311-318, 2015.

JAAFAR, N. I.; AJIS, A. Organizational Climate and Individual Factors Effects on Information Security Compliance Behaviour. **International Journal of Business and Social Science**, v.4, n.10, p.118-130, 2013.

JANCZEWSKI, L.; SHI, F. X. Development of information security baselines for healthcare information systems in New Zealand. **Computers & Security**, v.21, n.2, p.172-192, 2002.

JOHNSON, M. E.; GOETZ, E. Embedding information security into the organization. **IEEE Security & Privacy**, May/June, p.16-24, 2007.

JUNG, B.; HAN, I.; LEE, S. Security threats to internet: A Korean multi-industry investigation. **Information & Management**, v.38, p.487-498, 2001.

KANKANHALLI, A.; TEO, H.; TAN, B. C. Y.; WEI, K. An integrative study of information systems security effectiveness. **International Journal of Information Management**, v.23, n.2, p.139-154, 2003.

KATOS, V.; ADAMS, C. Modelling corporate wireless security and privacy. **Journal of Strategic Information Systems**, v.14, p.307-321, 2005.

KELLOWAY, E. K.; FRANCIS, L.; PROSSER, M.; CAMERON, J. E. Counterproductive work behavior as protest. **Human Resource Management Review**, v.20, n.1, p.18-25, 2010.

KRAEMER, S.; CARAYON, P. Human errors and violations in and information security: The viewpoint of network administrators and security specialists. **Applied Ergonomics**, v.38, p. 143-154, 2007.

KRAEMER, S.; CARAYON, P.; CLEM, J. Human and organizational factors in computer and information security: Pathways to vulnerabilities. **Computers & Security**, v.28, p.509-520, 2009.

KRUGER, H. A.; KEARNEY, W. D. A prototype for assessing information security awareness. **Computers & Security**, v.25, n.4, p.289-296, 2006.

KUO, F.; LIN, C. S.; HSU, M. Assessing gender differences in computer professional's self-regulatory efficacy concerning information privacy practices. **Journal of Business Ethics**, v.73, p.145-160, 2007.

KWANTES, C. T; BOGLARSKY, C. A. Perceptions of organizational culture, leadership effectiveness and personal effectiveness across six countries. **Journal of International Management**, v.13, n.2, p.204-230, 2007.

LACEY, D. **Managing the human factor in information security: How to win over staff and influence business managers**. West Sussex: John Wiley and Sons, 2009.

LACEY, D. Understanding and transforming organizational security culture. **Information Management & Computer Security**, v.18, n.1, p.4-13, 2010.

LEACH, J. Improving user security behaviour. **Computers & Security**, v.22, n.8, p. 685-692, 2003.

LEE, S. M.; LEE, S.; YOO, S. An integrative model of computer abuse based on social control and general deterrence theories. **Information & Management**, v.41, p.707-718, 2004.

LEONARD, L. N. K.; CRONAN, T. P.; KREIE, J. What influences IT ethical behavior intentions - Planned behavior, reasoned action, perceived importance, or individual characteristics? **Information & Management**, v.42, p.143-158, 2004.

LIGINLAL, D.; SIM, I.; KHANSA, L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. **Computers & Security**, v.28, p.215-228, 2009.

LOCH, K. D.; CARR, H. H.; WARKENTIN, M. E. Threats to information systems: Today's reality, yesterday's understanding. **MIS Quarterly**, June, p.173-186, 1992.

LUCIANO, E. M.; MAHMOOD, M. A.; MAÇADA, A. C. G. The influence of human factors on vulnerability to information security breaches. **Proceedings of the Sixteenth Americas Conference on Information Systems**, Lima, Peru, 2010.

MA, Q.; JOHNSTON, A. C.; PEARSON, J. M. Information security management objectives and practices: A parsimonious framework. **Information Management & Computer Security**, v.16, n.3, p.251-270, 2008.

MALHOTRA, N. **Pesquisa de marketing: uma orientação aplicada.** Porto Alegre: Bookman, 2006.

MANDARINI, M. **Segurança corporativa estratégica**. São Paulo: Manole, 2004.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2003.

MARCONI, M. A.; LAKATOS, E. M. **Técnicas de pesquisa**. São Paulo: Atlas, 2011.

MITTAL, N.; NAULT, B. R. Investments in information technology: Indirect effects and information technology intensity. **Information Systems Research**, V. 20, n.1, p.140-154, 2009.

NG, B.; KANKANHALLI A.; XU Y. Studying users' computer security behavior: A health belief perspective. **Decision Support Systems**, v.46, n.4, p.815-825, 2009.

OKENYI, P. O.; OWENS, T. J. On the anatomy of human hacking. **Information Systems Security**, v.16, p.302-314, 2007.

PAHNILA, S.; SIPONEN, M.; MAHMOOD, A. Which factors explain employees' adherence to information security policies? An empirical study. **Proceedings of the Eleventh Pacific Asia Conference on Information Systems**, Auckland, Nova Zelândia, 2007.

PAVLOU, P. A.; LIANG, H.; XUE, Y. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. **MIS Quarterly**, v.31, n.1, p.105-136, 2007.

PETERS, S. CSI computer crime & security survey 2009. **Computer Security Institute**, 2009.

PUCRS. Biblioteca Central Ir. José Otão. **Modelo de Referências Elaborado pela Biblioteca Central Irmão José Otão**. Disponível em: <http://www3.pucrs.br/portal/page/portal/biblioteca/Capa/BCEPesquisa/BCEPesquisaModelos>. Acesso em: 12 ago. 2014.

PUCRS. Biblioteca Central Ir. José Otão. **Modelo para apresentação de citações em documentos elaborado pela Biblioteca Central Irmão José Otão. 2011**. Disponível em: <http://www3.pucrs.br/portal/page/portal/biblioteca/Capa/BCEPesquisa/BCEPesquisaModelos>. Acesso em: 12 ago. 2014.

PUCRS. Biblioteca Central Ir. José Otão. **Modelo para apresentação de trabalhos acadêmicos, teses e dissertações elaborado pela Biblioteca Central Irmão José Otão**. 2011. Disponível em: <www.pucrs.br/biblioteca/trabalhosacademicos>. Acesso em: 12 ago. 2014.

PUHAKAINEN, P.; SIPONEN, M. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. **MIS Quarterly**, v.34, n.4, p.757-778, 2010.

PWC BRASIL. Pesquisa global sobre crimes econômicos 2011. **PricewaterhouseCoopers**, 2012.

PWC INTERNATIONAL. Pesquisa global de segurança da informação 2012. **PricewaterhouseCoopers**, 2011.

PWC INTERNATIONAL. Pesquisa global de segurança da informação 2013. **PricewaterhouseCoopers**, 2013.

RANSBOTHAM, S.; MITRA, S. Choice and chance: A conceptual model of paths to information security compromise. **Information Systems Research**, Articles in Advance, p.1-19, 2008.

REZGUI, Y.; MARKS, A. Information security awareness in higher education: An exploratory study. **Computers & Security**, v.27, p.241-253, 2008.

RICHARDSON, R. CSI computer crime & security survey 2008. **Computer Security Institute**, 2008.

ROESCH, S. M. A. **Projetos de estágio e de pesquisa em administração**: guia para estágios, trabalhos de conclusão, dissertações e estudos de caso. 3. ed. São Paulo: Atlas, 2009.

ROTVOLD, G. How to create a security culture in your organization. **Information Management Journal**, p.32-38, 2008.

SAMPIERI, R.; COLLADO, C.; LUCIO, P. **Metodologia de pesquisa**. São Paulo: McGraw-Hill, 2006.

SARKAR, K. R. Assessing insider threats to information security using technical, behavioural and organisational measures. **Information Security Technical Report**, v.15, p.112-133, 2010.

SÊMOLA, M. **Gestão da segurança da informação: Uma visão executiva**. Rio de Janeiro: Elsevier, 2003.

SHAW, R. S.; CHEN, C. C.; HARRIS, A. L.; HUANG, H. The impact of information richness on information security awareness training effectiveness. **Computers & Education**, v.52, p.92-100, 2009.

SIPONEN, M. A conceptual foundation for organizational information security awareness. **Information Management & Computer Security**, v.8, n.1, p.31-41, 2000.

SIPONEN, M. **Designing secure information systems and software: Critical evaluation of the existing approaches and a new paradigm.** Oulu: Oulu University Press, 2002.

SOLTANMOHAMMADI, S.; ASADI, S.; ITHNIN, N. Main human factors affecting information system security. **Interdisciplinary Journal of Contemporary Research in Business,** v.5, n.7, p.329-354, 2013.

SON, J.; KIM, S. S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. **MIS Quarterly**, v.32, n.3, p.503-529, 2008.

STANTON, J. M.; MASTRANGELO, P. R.; STAM, K. R.; JOLTON, J. Behavioral information security: Two end user survey studies of motivation and security practices. **Proceedings of the Tenth Americas Conference on Information Systems**, New York, EUA, 2004.

STRAUB, D.W. Effective IS security: An empirical study. **Information Systems Research**, v.1, n.3, p.255-276, 1990.

STRAUB, D. W.; WELKE, R. J. Coping with systems risk: Security planning models for management decision making. **MIS Quarterly**, v.22, n.4, p.441-469, 1998.

SUMNER, M. Information security threats: A comparative analysis of impact, probability and preparedness. **Information Systems Management**, v.26, p.2-12, 2009.

TRCEK, D.; TROBEC, R.; PAVESIC, N.; TASIC, J. F. Information systems security and human behavior. **Behaviour & Information Technology**, v.26, n.2, p.113-118, 2007.

VAAST, E. Danger is in the eye of the beholders: Social representations of information systems security in healthcare. **Journal of Strategic Information Systems**, v.16, p.130-152, 2007.

VAN NIEKERK, J. F.; VON SOLMS, R. Information security culture: A management perspective. **Computers & Security**, v.29, p.476-486, 2010.

VANCE, A.; SIPONEN, M.; PAHNILA, S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. **Information & Management**, v.49, p.190-198, 2012.

VENKATESH, W; MORRIS, M. G.; DAVIS, G. B.; DAVIS, F. D. User acceptance of Information Technology: toward a unified view. **MIS Quarterly,** v. 27, n. 3, p. 425-478, 2003.

VERGARA, S. C. **Métodos de coleta de dados no campo**. São Paulo: Atlas, 2012.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management. **Computers & Security**, v.23, p.371-376, 2004.

VROOM, C.; VON SOLMS, R. Towards information security behavioural compliance. **Computers & Security**, v.23, p.191-198, 2004.

WARD, P.; SMITH, C. L. The development of access control policies for information technology systems. **Computers & Security**, v.21, n.4, p.356-371, 2002.

WARKENTIN, M.; WILLISON, R. Behavioral and policy issues in information systems security: The insider threat. **European Journal of Information Systems**, v.18, p.101-105, 2009.

WILLIAMS, P. A. Information Security Governance. **Information Security Technical Report**, v.6, n.3 p. 60-70, 2001.

WILLIAMS, P. A. H. In a 'trusting' environment, everyone is responsible for information security. **Information Security Technical Report**, v.13, p.207-215, 2008.

WILSON, J. L.; TURBAN, E.; ZVIRAN, M. Information systems security: A managerial perspective. **International Journal of Information Management**, v.12, p.105-119, 1992.

WOOD, C. C.; BANKS, W. W. Human error: An overlooked but significant information security problem. **Computers & Security**, v.12, p.51-60, 1993.

WORKMAN, M.; BOMMER, W. H.; STRAUB, D. Security lapses and the omission of information security measures: A threat control model and empirical test. **Computers in Human Behavior**, v.24, p.2799–2816, 2008.

WULFF, C.; BERGMAN, L. R.; SVERKE, M. General mental ability and satisfaction with school and work: A longitudinal study from ages 13 to 48. **Journal of Applied Developmental Psychology**, Article in Press, 2009.

YIN, R. K. **Estudo de caso**: planejamento e métodos. Porto Alegre: Bookman, 2007.

APÊNDICE A – ROTEIRO DE ENTREVISTAS

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

Prezado(a) Senhor(a)

Esta pesquisa aborda o tema Segurança da Informação, especificamente os contextos organizacional e de Tecnologia e Segurança da Informação e suas influências no comportamento responsável dos colaboradores visando evitar vulnerabilidades relacionadas a ameaças internas de Segurança da Informação. Este roteiro de entrevistas é parte integrante da dissertação do mestrando Ruy Carlos Gomes Dini (ruycarlos.dini@gmail.com) do Mestrado em Administração e Negócios da PUCRS, orientado pela Profª. Drª. Edimara Mezzomo Luciano (eluciano@pucrs.br), do Programa de Pós-Graduação em Administração da PUCRS. Todas as informações prestadas pelos entrevistados são consideradas confidenciais. Portanto, não será divulgado o nome do entrevistado ou o nome da empresa na pesquisa.

Agradecemos o seu aceite em nos receber para esta entrevista.

1 – ENTREVISTA

Operacionalização:

Entrevista com CIO ou responsável pela Segurança da Informação.

1.1 - Questões semi-estruturadas

Serão aplicadas as questões referidas abaixo, a fim de obter maiores conhecimentos sobre os assuntos abordados nesta pesquisa. As respostas devem considerar o contexto da empresa na qual o respondente trabalha atualmente e sua experiência com Segurança da Informação.

1. Os funcionários têm conhecimento e habilidades suficientes que influenciam no comportamento responsável relativo à Segurança da Informação?

2. A experiência e o conhecimento geral do funcionário em Tecnologia da Informação influenciam no comportamento responsável relativo à Segurança da Informação?

3. O conhecimento da política de Segurança da Informação e seus efeitos práticos no dia a dia têm influência no comportamento responsável relativo à Segurança da Informação?

4. A severidade da política de Segurança da Informação influencia no comportamento responsável relativo à Segurança da Informação?

5. Os mecanismos de controle da Segurança da Informação estão relacionados com a inibição do desempenho e da criatividade do funcionário, no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?

6. O que a empresa faz quando um funcionário viola regras e normas que podem gerar vulnerabilidades a ameaças internas de Segurança da Informação? Se ele for reincidente, há controles adicionais, no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?

7. A punição contribui para inibir a reincidência de erros no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?

8. A organização monitora as atividades dos funcionários no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?

9. Você considera que o monitoramento consciente pode inibir, coagir ou acuar os funcionários no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?

10. O clima organizacional influencia no comportamento responsável relativo à Segurança da Informação?

11. Um grande volume de procedimentos e práticas de Segurança da Informação interfere no fluxo de trabalho, a ponto de influenciar no comportamento responsável relativo à Segurança da Informação?

12. A cultura organizacional influencia no comportamento responsável relativo à Segurança da Informação?

13. O relacionamento entre os funcionários e seus superiores pode influenciar no comportamento responsável relativo à Segurança da Informação?

14. As condições de trabalho podem influenciar no comportamento responsável relativo à Segurança da Informação?

15. Diferentes ambientes organizacionais (ambientes cooperativos e ambientes competitivos) podem influenciar no comportamento responsável relativo à Segurança da Informação de maneira diferenciada?

16. O comportamento responsável dos funcionários relativo à Segurança da Informação é influenciado por colegas de trabalho?

17. A satisfação do funcionário com o trabalho pode influenciar no comportamento responsável relativo à Segurança da Informação?

18. Onde e de que maneira a empresa deixa claro qual é o comportamento desejável no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?

19. A empresa possui programas de treinamento, capacitação e/ou conscientização periódicos que visam evitar vulnerabilidades a ameaças internas de Segurança da Informação? É possível perceber se existe relação destes programas no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?

20. Um funcionário, ao atender somente a política de Segurança da Informação, estará contribuindo no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?

21. Espera-se que o funcionário faça somente o que está expresso como permitido na política de Segurança da Informação ou considera-se adequado situações concretizadas que não foram contempladas dentro da política, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?

22. Não importa o quão pequeno seja, violar as regras e normas é um assunto sério e merece punição, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?

23. Podem-se violar as regras e normas, se ninguém for prejudicado, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?

24. Violar as regras e normas pode ser legítimo, se for para obter produtividade, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?

25. É possível perceber alguma relação entre o gênero do funcionário e o comportamento responsável em relação à Segurança da Informação?

26. A lealdade de um funcionário à empresa está relacionada com o comportamento responsável relativo à Segurança da Informação?

27. O nível de escolaridade do funcionário está relacionado com o comportamento responsável em relação à Segurança da Informação?

28. O nível hierárquico ou o cargo do funcionário está relacionado com o comportamento responsável em relação à Segurança da Informação?

1.2 - Questões Sócio-demográficas

Questões que buscam caracterizar o perfil da empresa e do respondente.

1. Quantos funcionários trabalham na empresa no Brasil?

2. Aproximadamente quantos funcionários utilizam computadores na empresa?

3. Aproximadamente qual é o percentual do faturamento investido em TI?

4. A empresa está sujeita a regulatórios (como regras da CVM ou Sarbanes-Oxley)? Em caso positivo, quais?

5. Quantos anos de experiência você possui na área de TI?

6. Há quanto tempo você desempenha sua atual função na empresa?

APÊNDICE B - DIMENSÕES, VARIÁVEIS E QUESTÕES

DIMENSÕES		VARIÁVEIS	QUESTÕES	PRINCIPAIS FONTES
Contexto de Tecnologia e Segurança da Informação	Entendimento sobre TI e Segurança da Informação	Conhecimento e Habilidades	1. Os funcionários têm conhecimento e habilidades suficientes que influenciam no comportamento responsável relativo à Segurança da Informação?	Workman, Bommer e Straub (2008)
		Experiência e Conhecimentos Gerais em TI	2. A experiência e o conhecimento geral do funcionário em Tecnologia da Informação influenciam no comportamento responsável relativo à Segurança da Informação?	Lacey (2009)
		Conhecimento da Política de Segurança da Informação	3. O conhecimento da política de Segurança da Informação e seus efeitos práticos no dia a dia têm influência no comportamento responsável relativo à Segurança da Informação?	Lee, Lee e Yoo (2004)
		Severidade da Política de Segurança da Informação	4. A severidade da política de Segurança da Informação influencia no comportamento responsável relativo à Segurança da Informação?	Herath e Rao (2009a)
	Controles e Punições	Mecanismos de Controle como Inibidores do Desempenho e da Criatividade	5. Os mecanismos de controle da Segurança da Informação estão relacionados com a inibição do desempenho e da criatividade do funcionário, no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?	O autor (2014)
		Mecanismos de Controle da Violação de Regras e Normas	6a. O que a empresa faz quando um funcionário viola regras e normas que podem gerar vulnerabilidades a ameaças internas de Segurança da Informação? 6b. Se ele for reincidente, há controles adicionais, no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?	O autor (2014)
		Punição como Inibidor da Reincidência de Eventos de Segurança da Informação	7. A punição contribui para inibir a reincidência de erros no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?	Herath e Rao (2009a)
		Monitoramento	8. A organização monitora as atividades dos funcionários no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?	D'Arcy, Hovav e Galletta (2008) e Herath e Rao (2009a)
		Monitoramento como Inibidor de Eventos de Segurança da Informação	9. Você considera que o monitoramento consciente pode inibir, coagir ou acuar os funcionários no sentido de influenciar no comportamento responsável relativo à Segurança da Informação?	D'Arcy, Hovav e Galletta (2008) e Herath e Rao (2009a)
Contexto Organizacional		Clima Organizacional	10. O clima organizacional influencia no comportamento responsável relativo à Segurança da Informação?	Chan, Woon e Kankanhalli (2005)
		Fluxo de Trabalho de Segurança da Informação	11. Um grande volume de procedimentos e práticas de Segurança da Informação interfere no fluxo de trabalho, a ponto de influenciar no comportamento responsável relativo à Segurança da Informação?	Albrechtsen (2007)
		Cultura Organizacional	12. A cultura organizacional influencia no comportamento responsável relativo à Segurança da Informação?	Chang e Lin (2007)
		Relação entre Funcionários e seus Superiores	13. O relacionamento entre os funcionários e seus superiores pode influenciar no comportamento responsável relativo à Segurança da Informação?	Vroom e Von Solms (2004) e Shaw *et al*. (2009)
		Condições de Trabalho	14. As condições de trabalho podem influenciar no comportamento responsável relativo à Segurança da Informação?	Bozionelos (2001) e Kelloway *et al*. (2010)
		Diferenças entre Ambientes Organizacionais	15. Diferentes ambientes organizacionais (ambientes cooperativos e ambientes competitivos) podem influenciar no comportamento responsável relativo à Segurança da Informação de maneira diferenciada?	Mikkelsen (2002) e Dulebohn (2009)
		Comportamento dos Pares	16. O comportamento responsável dos funcionários relativo à Segurança da Informação é influenciado por colegas de trabalho?	Herath e Rao (2009a)
		Satisfação com o Trabalho	17. A satisfação do funcionário com o trabalho pode influenciar no comportamento responsável relativo à Segurança da Informação?	Stanton *et al*. (2004)

DIMENSÕES	VARIÁVEIS	QUESTÕES	PRINCIPAIS FONTES
Comportamento Responsável Relativo à Segurança da Informação	Disseminação do Comportamento	18. Onde e de que maneira a empresa deixa claro qual é o comportamento desejável no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?	O autor (2014)
	Treinamento, Capacitação e Conscientização	19a. A empresa possui programas de treinamento, capacitação e/ou conscientização periódicos visando evitar vulnerabilidades a ameaças internas de Segurança da Informação? 19b. É possível perceber se existe relação destes programas no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?	Lee, Lee e Yoo (2004)
	Política de Segurança da Informação como Mecanismo de Proteção	20. Um funcionário, ao atender somente a política de Segurança da Informação, estará contribuindo no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?	O autor (2014)
	Juízo de Comportamento Relacionado à Política de Segurança da Informação	21. Espera-se que o funcionário faça somente o que está expresso como permitido na política de Segurança da Informação ou considera-se adequado situações concretizadas que não foram contempladas dentro da política, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?	O autor (2014)
	Seriedade da Violação de Regras e Normas	22. Não importa o quão pequeno seja, violar as regras e normas é um assunto sério e merece punição, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?	Lee, Lee e Yoo (2004)
	Prejudicialidade da Violação de Regras e Normas	23. Podem-se violar as regras e normas, se ninguém for prejudicado, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?	Lee, Lee e Yoo (2004)
	Legitimidade da Violação de Regras e Normas	24. Violar as regras e normas pode ser legítimo, se for para obter produtividade, no sentido de evitar vulnerabilidades a ameaças internas de Segurança da Informação?	Lee, Lee e Yoo (2004)
Moderadores do Comportamento Responsável	Gênero	25. É possível perceber alguma relação entre o gênero do funcionário e o comportamento responsável em relação à Segurança da Informação?	O autor (2014)
	Lealdade à Empresa	26. A lealdade de um funcionário à empresa está relacionada com o comportamento responsável relativo à Segurança da Informação?	Lacey (2009)
	Escolaridade	27. O nível de escolaridade do funcionário está relacionado com o comportamento responsável em relação à Segurança da Informação?	O autor (2014)
	Nível Hierárquico	28. O nível hierárquico ou o cargo do funcionário está relacionado com o comportamento responsável em relação à Segurança da Informação?	O autor (2014)