UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO

LUCIANA EMIRENA DOS SANTOS CARNEIRO

GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO NO ÂMBITO DAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO: PESSOAS, PROCESSOS E TECNOLOGIA

Belo Horizonte
2012

LUCIANA EMIRENA DOS SANTOS CARNEIRO

GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO NO ÂMBITO DAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO: PESSOAS, PROCESSOS E TECNOLOGIA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Escola de Ciência da Informação da Universidade Federal de Minas Gerais para obtenção do grau de Mestre em Ciência da Informação.
Linha de Pesquisa: Organização e Uso da Informação
Orientador: Prof. Dr. Maurício Barcellos Almeida

BELO HORIZONTE

2012

Carneiro, Luciana Emirena dos Santos.

C289g Gestão da informação e do conhecimento no âmbito das práticas de segurança da informação [manuscrito] : pessoas, processos e tecnologia / Luciana Emirena dos Santos Carneiro. – 2012.
258 f. : il., enc.

Orientador: Maurício Barcellos Almeida.
Dissertação (mestrado) – Universidade Federal de Minas Gerais, Escola de Ciência da Informação.
Referências: f. 245-253
Anexos: f. 254-258

1. Ciência da informação – Teses. 2. Segurança da informação – Teses. 3. Gestão do conhecimento – Teses. 4. Sistemas de informação gerencial – Teses. 5. Comportamento informacional – Teses. 6. Política informacional – Teses. I. Título. II. Almeida, Maurício Barcellos. III. Universidade Federal de Minas Gerais, Escola de Ciência da Informação.

CDU: 659.2

Ficha catalográfica: Biblioteca Profª Etelvina Lima, Escola de Ciência da Informação da UFMG

Universidade Federal de Minas Gerais
Escola de Ciência da Informação
Programa de Pós-Graduação em Ciência da Informação

Dissertação intitulada Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: Pessoas, Processos e Tecnologias, de autoria de Luciana Emirena dos Santos Carneiro, aprovada pela banca examinadora constituída pelos seguintes professores:

_____

Prof. Dr. Maurício Barcellos Almeida
Universidade Federal de Minas Gerais

_____

Profª. Drª. Beatriz Valadares Cendón
Universidade Federal de Minas Gerais

_____

Prof. Dr. Renato Rocha Souza
Fundação Getúlio Vargas do Rio de Janeiro

_____

Profª. Drª. Renata Maria Abrantes Baracho Porto
Coordenadora do Programa de Pós-Graduação em Ciência da Informação - PPGCI ECI/UFMG

Data de aprovação: Belo Horizonte, 20 de dezembro de 2012.

AGRADECIMENTOS

Quando tomei a decisão de buscar esse sonho, havia eu, meu sonho, uma ideia e mais nada. Mas algo falava alto no meu peito, uma voz forte, essa voz sempre me dizia para seguir em frente, para tentar o mestrado.

Enchi o peito de coragem, enfrentei todos aqueles que, num primeiro momento, pensavam que eu estava fazendo a escolha errada e iniciei o desenvolvimento do meu projeto de mestrado.

Desenvolvi o projeto, fiz as provas do concurso do mestrado e passei. Nem eu mesma acreditava quando li meu nome na lista dos candidatos selecionados. Nossa quanta emoção! Meu Deus, eu, enfim, era aluna da ECI - UFMG! Nossa quanta honra!

Por me manter firme, por não me deixar esmorecer, desaminar, desistir ou vacilar eu agradeço à Deus. Foi ELE quem me proveu de forças e era ELE, a voz que falava ao meu coração e dizia “vai Luciana, coragem, você é capaz”!

Deus também colocou no meu caminho o meu mestre, o Prof. Dr. Maurício Barcellos Almeida, a quem devo meus mais sinceros agradecimentos. Foi ele quem acreditou naquele projeto de segurança da informação, escrito de forma simplória, e, que hoje se tornou uma dissertação! Professor Maurício, jamais vou me esquecer de seus ensinamentos, de sua paciência, de sempre instigar em nós mesmos a busca por uma forma de expressão mais simples de ser entendida pelo leitor, por dividir comigo seus conhecimentos, por me acolher, me escutar, me elogiar, me motivar e sempre me dedicar muita atenção e respeito. Obrigada! Levo do nosso tempo de convívio as melhores recordações! Você é o melhor! Como já te disse várias vezes o seu SIM mudou a minha vida, Mais uma vez obrigada!

Continuando a minha história, quando fiz a minha matrícula e iniciei a minha trajetória na qualidade de mestranda, contei com vários torcedores. Minha mãe - Maria, meus irmãos – Lin, Nado e Luiz e minhas madrinhas – Zizi e Maria Helena eram puro orgulho! Quero nesse momento relembrar alguns casos e agradecer por terem entendido algumas ausências de minha parte lá em casa, por terem torcido, rezado, se preocupado, conversado comigo, por sempre me perguntarem “e aí Luciana como está a dissertação?”, “minha filha acabou a dissertação?”, por terem me ouvido, me aconselhado, me entendido e me amado. Lembro-me de minha mãe na porta do jardim quando eu era criança, me esperando porque eu chorava sem parar por não querer ir à escola... Lembro também das idas dela para me levar à escola, de sentar para fazer as

tarefas comigo. Outro dia, semana passada, na defesa da minha irmã, mamãe disse que realiza em seus filhos o sonho que tinha de ser professora. Mãe, faço sua essa conquista! Não me esqueço também das idas todas as tardes à casa de minhas tias para estudar, do curso de inglês – obrigada! Outro agradecimento público, faço ao meu irmão Nado, que lutou muito para eu tivesse um ensino médio de qualidade e conseguiu uma bolsa para mim no Colégio Arquidiocesano, Obrigada Nado! Meu muito obrigada à todos meus familiares, o esforço de todos vocês permitiu que eu chegasse hoje até aqui e conquistasse algo tão especial! Obrigada! Amo vocês! Muito Obrigada!

Não posso deixar que fazer um agradecimento especial a minha irmã Lílian, minha melhor amiga. Li, você é uma pessoa formidável! Obrigada por ter me ajudado, por ter lido esboços de artigos, de capítulos de dissertação, por ter me aconselhado e me ajudado, por me dar seu ombro amigo, por me ouvir, me entender. Obrigada pela sua amizade, que é serena, doce, sem censuras e nem reservas, que me entende e me aceita do jeito que eu sou e que me ama incondicionalmente. Eu também te amo muito!

É também momento de agradecer o meu marido – Reinaldo. Quantas vezes você ouviu a leitura da dissertação em voz alta, hein amor?!? Quero dizer muito obrigada por acreditar no meu sonho, por ter me apoiado nesse tempo no qual fui bolsista CAPES, por vibrar comigo na conquista das publicações, por ter sido parceiro, amigo, por ter entendido algumas ausências em momentos que sei que você gostaria da minha presença, por ter me amado e me encorajado. Muito obrigada! Hoje sentimos aquele gostinho delicioso de dever cumprido! Essa dissertação também é sua! Te amo!

Agradeço também à Escola de Ciência da Informação da UFMG, meus professores e os funcionários desta escola que me acolheram com carinho e me ajudaram a trilhar os primeiros passos na carreira de docente. Aqui aprendi o que é ser docente, com incríveis exemplos que jamais vou esquecer – Prof. Renato, Profª. Marta, Profª Mônica, Profª. Beatriz, Prof. Ricardo, Prof. Cláudio, Prof. Casal, Profª. Marta Ferreira, Profª. Gercina e tantos outros que igualmente contribuíram para meu crescimento pessoal e profissional! Obrigada!

Certa vez, quando pretendia ingressar na especialização em gestão estratégica da informação, o Prof. Renato e a Profª. Marta vieram fazer a entrevista, que é parte do processo seletivo, e ouviram de mim que era um sonho antigo estudar na UFMG e que a especialização era meu pontapé inicial. Viram como era verdade?! E não pretendo parar por aqui!

Faço um agradecimento muito especial à PUC MG, primeira universidade que me contratou como docente, aos meus alunos e aos professores Nivaldo Miranda, Profª Beatriz Magalhães Gomes, Walter Tedeschi, Ronaldo Rodrigues e Rosilene Rocha Martins. Aos professores, meus colegas de trabalho, agradeço pela credibilidade, por terem confiado em mim e pela oportunidade. Vocês com muito amor vem me ensinando os caminhos da docência e afastando de mim os espinhos que surgem. Vocês fazem com que meu caminhar seja doce e leve! Agradeço à Deus por terem colocado vocês na minha vida! Obrigada, de coração obrigada!

Agora é a vez de agradecer aos meus alunos, a minha sustentação! Meus amados alunos, muito obrigada por permitirem que eu participe do crescimento de vocês! Eu que me sinto muito honrada por me deixarem participar da construção profissional de cada um de vocês. Obrigada pelo carinho, pelo respeito e pela confiança! É uma alegria ter podido conviver com cada de vocês! Posso dizer com toda convicção que vocês serão profissionais de muito sucesso! Como disse várias vezes vocês são meus rouxinóis e estão prontos para voar, voar alto, romper o novo e os desafios e se tornarem profissionais de muito sucesso no mercado. Vocês são ousados, criativos, tem garra, brilho nos olhos e vontade de vencer! Profissionais que vão agregar e muito com seu jeito inovador no mercado de trabalho. Sei que um dia se lembrarão com muito carinho de tudo que vivemos e como foi bom! Vocês marcaram a minha história e hoje estão aqui compartilhando um dos momentos mais especiais da minha vida comigo! Obrigada amados!

Alguns torcedores vibraram tanto com a minha conquista e me incentivaram tanto que como gostaria que estivessem aqui para brindar comigo essa vitória.... mas Deus fez planos diferentes. E apesar de hoje não poder contar com sua presença mais entre nós, quero agradecer à minha prima-irmã Rizza, que sempre me incentivou e que não via a hora da defesa chegar. Um dos nossos planos era montar uma transmissão online haja vista que ela residia na Suiça e ainda não sabia se poderia estar presente no dia de hoje. Outra pessoa que não posso deixar agradecer é ao Sérgio, meu cunhado. Ele era um entusiasta do tema segurança da informação e em sua última visita à minha casa aqui em Belo Horizonte conversamos muito sobre o tema. Ele também era outro que gostaria muito de estar aqui nesse dia especial.

Não posso deixar de me lembrar do meu pai que tenho certeza que estaria muito orgulhoso de ter uma filha mestra!

Durante o período que convivi aqui na UFMG fiz muito amigos. Pessoas com as quais dividimos angústias, ansiedades, trabalhos, tarefas, opiniões, risos, conselhos e que se tornaram amigos, amigos queridos e presentes! Não posso deixar de dar o meu muito obrigada aos amigos Ariane, Joel, Lívia, Paula, Lílian, Ráisa, Joice, Flavinha, Fátima, Juliana, Rafael e Ranito. Obrigada pela amizade e pelo carinho de sempre!

Aos meus amigos – Camila, Mirela, Luciana Gonçalves, Suellen, Lucimara, Tiago Jorge, Zanon, Yasmim (valeu pela força com o Prezi) e à D. Nely – minha sogra incentivadora, e, tantos outros amigos que não conseguirei nominar aqui, se não a lista ficará muito grande, agradeço imensamente as conversas, os conselhos, o conhecimento compartilhado, o convívio, as risadas, a compreensão e as conversas! Muito obrigada!

Hoje finalizo essa etapa, e escrevo mais uma página da minha história. Com certeza saio daqui uma pessoa muito diferente de quando entrei. Levo comigo um pouco mais de bagagem, de responsabilidade e certa de que nasci para ser pesquisadora e docente! Onde for levarei comigo o compromisso de compartilhar o que aprendi nessa maravilhosa escola e honrar o nome da Escola de Ciência da Informação e da UFMG. Muito obrigada por tudo!

"Nada posso lhe oferecer que não exista em você mesmo. Não posso abrir-lhe outro mundo além daquele que há em sua própria alma. Nada posso lhe dar, a não ser a oportunidade, o impulso, a chave. Eu o ajudarei a tornar visível o seu próprio mundo, e isso é tudo." (Hesse)

RESUMO

Propósito: A presente pesquisa tem a intenção de investigar a inter-relação entre o elemento humano e a segurança da informação no contexto corporativo visando explorar como, por que e em quais circunstâncias ocorrem falhas de segurança que envolvem pessoas e entender como lidar com elas.

Abordagem / Metodologia: A proposta é desenvolver um estudo quali-quantitativo, no âmbito das Ciências Sociais Aplicadas, que venha a contribuir para esclarecer a interferência do elemento humano na segurança da informação. Busca-se identificar os perfis dos usuários que possuam inter-relação com falhas de segurança, entender com qual frequência são usados dispositivos tecnológicos que possam gerar perda de informação que tenha valor para a empresa, identificar circunstâncias nas quais as falhas de segurança ocorrem, a natureza dos incidentes de segurança informacional e suas razões.

Resultados: Da avaliação dos dados, pode-se concluir que o elemento pessoas é uma variável crítica na gestão de segurança informacional nas organizações. As políticas de informação devem ser acessíveis aos funcionários e factíveis de serem executadas. Com relação à tecnologia, é valido que continuem os investimentos, entretanto eles devem ser equilibrados com o desenvolvimento de controles informais (pessoas) e controles formais (políticas e processos) para que haja uma gestão de segurança informacional mais efetiva e eficaz.

Palavras-chave: Segurança da informação; Políticas de informação; Comportamento Informacional; Sistemas de Informação; Gestão da Informação e do Conhecimento.

ABSTRACT

Purpose: This study intends to investigate the interrelation between the human element and the information security in the corporate context, in order to analyze how, why and in which circumstances security failures, that involve people, happen, and also to understand how to deal with them.

Approach/Methodology: The proposal is to develop a quali-quantitative study, within the scope of Applied Social Sciences, which may contribute to clarify the interference of the human element in the information security. The aim is to identify user profiles with interrelation with security failures, to understand how frequently technological devices, that may generate loss of information that has value to the company, are used, to find situations in which security failures occur, the nature of security incidents and their reason.

Results: From the evaluation of the data, it was possible to conclude that the "people" element is a critical variable in the informational security management of the organizations. The information policies must be accessible to the employees and possible to be executed. In relation to the technology, it is valid to continue the investments, however they must be balanced with the development of informal controls (people) and formal controls (policies and procedures) so as the informational security management becomes more effective and efficient.

Keywords: Information Security; Information Policy; Informational Behavior; Information Systems; Information and knowledge Management

LISTA DE TABELAS

Tabela 1 199
Tabela 2 203
Tabela 3.....209
Tabela 4.....,.....210
Tabela 5.....,.....211
Tabela 6 214
Tabela 7.....215
Tabela 8.....,.....216
Tabela 9.....,.....218
Tabela 10 219
Tabela 11 219
Tabela 12 221
Tabela 13 222
Tabela 14 223
Tabela 15 224
Tabela 16 225
Tabela 17 .....,.....226
Tabela 18 227
Gráfico 1 217
Gráfico 2 229
Gráfico 3 .....,.....232
Gráfico 4 234
Gráfico 5 237
Gráfico 4.....240

LISTA DE QUADROS

Quadro 1 119
Quadro 2 125
Quadro 3 129
Quadro 4.....133
Quadro 5.....137
Quadro 6.....140
Quadro 7.....146
Quadro 8.....150
Quadro 9.....154
Quadro 10.....158
Quadro 11.....163
Quadro 12.....166
Quadro 13.....170
Quadro 14.....173
Quadro 15.....176
Quadro 16.....180
Quadro 17.....183
Quadro 18.....186
Quadro 19.....190
Quadro 20.....193

LISTA DE ABREVIATURAS

SI	–	SEGURANÇA DA INFORMAÇÃO
GI	-	GESTÃO DA INFORMAÇÃO
GC	-	GESTÃO DO CONHECIMENTO

SUMÁRIO

1 INTRODUÇÃO 17

2 VISÃO PRELIMINAR SOBRE A SEGURANÇA DA INFORMAÇÃO: DEFINIÇÕES E ABRANGÊNCIA DA SEGURANÇA DA INFORMAÇÃO 24

3 SEGURANÇA DA INFORMAÇÃO: PERSPECTIVAS DE ESTUDOS EM CIÊNCIA DA INFORMAÇÃO 36

3.1 – PESSOAS E SEGURANÇA DA INFORMAÇÃO: ABORDAGENS PRELIMINARES 47

3.1.1- SEGURANÇA DA INFORMAÇÃO E GESTÃO DE RECURSOS HUMANOS: PERSPECTIVAS DE MODELAGENS GERENCIAIS 48

3.2 - SEGURANÇA E RECURSOS ORGANIZACIONAIS 75

3.2.1 SEGURANÇA DA INFORMAÇÃO E PROCESSOS – ABORDAGEM NO CONTEXTO DAS POLÍTICAS DE INFORMAÇÃO 75

3.3– A SEGURANÇA DA INFORMAÇÃO E OS SISTEMAS 89

3.3.1 SEGURANÇA DA INFORMAÇÃO E TECNOLOGIA – PERSPECTIVAS DE DISCUSSÃO NO CONTEXTO DA CIÊNCIA DA INFORMAÇÃO 90

4- METODOLOGIA DE PESQUISA 102

4.1 FINS DA PESQUISA, MEIOS DE INVESTIGAÇÃO E RACIOCÍNIO LÓGICO DA PESQUISA 103

4.2 TIPOS E PROCEDIMENTOS DA PESQUISA – APLICAÇÃO PRÁTICA 104

4.2.1 SELEÇÃO DO CASO: SUJEITOS, LOCAL DE PESQUISA, PLANO DE RECRUTAMENTO 105

4.2.2 DIAGNÓSTICO: COLETA DE DADOS DOCUMENTAIS E DADOS DO QUESTIONÁRIO 105

4.2.3 A CONSTRUÇÃO DO INSTRUMENTO DE COLETA DE DADOS 107

4.2.4 - METODOLOGIA PARA ANÁLISE DE DADOS 108

4.2.5 VALIDAÇÃO DO INSTRUMENTO DE COLETA DE DADOS 111

4.2.6 MAPEAMENTO DAS FONTES PRIMÁRIAS: ANÁLISE DESCRITIVA DOS DADOS 113

5- IMPLEMENTAÇÃO DA METODOLOGIA – RESULTADOS 116

5.1 – SELEÇÃO DO CASO: SUJEITOS, LOCAL DE PESQUISA, TIPO DE AMOSTRA E PLANO DE RECRUTAMENTO 116

5.2- ANÁLISE DOCUMENTAL E DOS DADOS PRIMÁRIOS ADVINDOS DO QUESTIONÁRIO 117

5.2 – INSTRUMENTO DE COLETA DE DADOS 197

5.2.1 – IMPLEMENTAÇÃO DA METODOLOGIA PARA ANÁLISE DOS DADOS: TABULAÇÃO DOS DADOS DO QUESTIONÁRIO 198

5.3 – VALIDAÇÃO DO INSTRUMENTO DE COLETA DE DADOS 206

5.3.1 – VALIDAÇÃO NOMOLÓGICA OU DE CONTEÚDO 207

5.3.2 – CONFIABILIDADE 208

5.3.3 – CAPACIDADE DE GENERALIZAÇÃO 211

5.4 – ANÁLISE DESCRITIVA DOS DADOS 216

6 - DISCUSSÃO DOS RESULTADOS 228

6.1 - CENÁRIO DE ASPECTOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO ... 228

6.2 - CENÁRIO COMPORTAMENTAL DOS COLABORADORES 235

6.3 - CENÁRIO DE DÉFICIT COMUNICACIONAL 238

6.4 - CENÁRIO DE INFORMAÇÕES RELATIVAS À TECNOLOGIA 239

7 - CONSIDERAÇÕES FINAIS 242

8 – REFERÊNCIAS BIBLIOGRÁFICAS: 245

9 - ANEXOS 254

1 Introdução

Informação, por si só, é um termo de difícil definição. Por sua complexidade, o assunto vem sendo abordado por estudiosos diversos. No século passado, a Ciência da Informação tomou para si tal responsabilidade, propondo uma abordagem abrangente que envolve tanto questões sociais quanto questões relacionadas a novas tecnologias. Por possuir esse perfil de considerar importantes questões de diversos ângulos, a Ciência da Informação tem se apresentado com um campo de pesquisa frutífero, cujos desafios são constantes.

A gestão da informação e do conhecimento se concretiza no cenário organizacional como subárea da Ciência da Informação, atuando diretamente nas corporações, devido ao fato da informação ter se tornado um ativo de grande valor para elas. Mesmo que esse fato seja objeto de discussões acaloradas e às vezes passionais, (Perelman, 1963), a evidência empírica demonstra que, de fato, algo mudou. Não que a informação e o conhecimento não fossem ambos importantes desde sempre para as organizações, mas sim o fato de que são diferentes as formas de armazenamento, disseminação, recuperação e valoração. A importância inerente aos elementos de busca, criação, compartilhamento e utilização das informações e do conhecimento nas organizações é inquestionável, haja vista o cenário econômico-político-social de intensa competitividade, globalização e acelerado desenvolvimento tecnológico.

A internet, a difusão da web, as redes, e, a presença cada vez mais marcante das tecnologias na vida das pessoas e nas organizações tem provocado profundas transformações e acelerações nos processos intrínsecos às rotinas pessoais e organizacionais. O grande avanço tecnológico favorece a conectividade, o compartilhamento, o encurtamento das distâncias geográficas, acessibilidade, mobilidade, dentre outros. É através do ambiente virtual e da velocidade de acesso permitida pelas redes que ocorre a interligação dos meios internos e externos, com eficiência e eficácia incomuns até os anos de 1980. Ressalva-se que o elemento “conhecimento”, obteve nova perspectiva a partir do desenvolvimento e da consolidação dos ambientes virtuais, haja vista que a rede viabiliza o acesso a conteúdos informatizados, renovando as possibilidades de circulação e acesso remoto a informações.

Em contrapartida, a facilidade no acesso à informação resultou, principalmente, em questões de obsolescência dos instrumentos antes utilizados para organizar a informação, na necessidade de lidar com volumes de dados até então inimagináveis e de selecionar os dados que serão úteis em grandes repositórios. Ao olhar a informação nessa vertente do cenário social, percebe-se a evolução das abordagens sobre o tema alterando a visão que antes era relativa à gestão de estoques de informação, passando para a perspectiva de como a informação se tornou agente de transformação da vida dos indivíduos, havendo assim a necessidade de estabelecer novos parâmetros de gestão e, desta vez, com o indivíduo no centro do processo.

A disponibilidade da informação para usuários é uma característica marcante na pretensa, assim chamada, Sociedade da Informação e traz consigo inúmeros benefícios, mas também grandes preocupações, como por exemplo, a insegurança dos ativos informacionais.

Assim, a crescente evolução e adequação dos sistemas de informação no cenário sócio-organizacional mundial possibilitou às empresas ganhos com mobilidade, inteligência e real capacidade de gestão. O aumento da competitividade e da descentralização promovido pelos avanços tecnológicos gera a necessidade de gestão, controle, segurança da informação e a proteção do conhecimento crítico (SIANES, 2006). As organizações passaram a demandar por tecnologias que viessem a garantir aos negócios a confidencialidade, integridade e disponibilidade, fazendo com que a segurança da informação passasse a ser uma estratégia de gestão da informação aplicável a toda organização (WYLDER (2004); KOSKOSAS, CHARITOUDI & LOUTA, (2008); SOLMS (2008); KRAEMER, CARAYON E CLEM (2009); GHERNAOUTI-HELIE (2009); COLWILL (2010); PREECE (2010)).

> Considera-se como premissa básica que os recursos humanos são o centro de todo o processo informacional e que são as pessoas que orientam o comportamento informacional da organização [...] destacando a necessidade do desenvolvimento de uma cultura organizacional voltada para a segurança da informação e para a proteção de conhecimentos relevantes, dos quais as organizações dependem para conquistar e manter suas vantagens competitivas (SIANES, 2006, p.255).

Na atualidade, os investimentos em segurança da informação são crescentes, como de fato as tecnologias da informação conseguem solucionar parte do problema diminuindo as ameaças físicas ou virtuais frente a pessoas ou informações que estas

possuem. Almeida (2007) ratifica esse posicionamento, colocando que a expressão segurança da informação representa um conceito amplo que, geralmente, nas empresas e instituições, está associada a sistemas informatizados e aos dados que estes manipulam.

Em contrapartida observou-se que por mais investimentos que se faça em segurança, se o elemento humano não for devidamente considerado, falhas de segurança ocorrerão (COLWILL, 2010). Solms (2008) ressalta que qualquer investimento em tecnologia não terá a eficiência esperada se os usuários não obtiverem uma consciência de Segurança Informacional. Complementar a essa visão é o posicionamento de SVEEN, TORRES & SARIEGI (2009), quando advogam uma abordagem para tratar a segurança da informação a partir de uma perspectiva de qualidade holística na melhoria de processos. Os investimentos em controles técnicos devem ser equilibrados com os investimentos na educação formal, bem como nos controles formais e informais, com atenção especial dada à criação de conhecimento nos processos.

Como, de fato, não se trata de enfatizar apenas alguns elementos que envolvem o processo de segurança da Informação. Uma abordagem bem fundamentada abarca as mais variadas áreas do contexto organizacional, além dos recursos computacionais, humanos, de infraestrutura, de logística, de comunicação, dentre outros. Nesse aspecto, ressalta-se que uma vez percebida nas dimensões organizacionais, pode-se detectar a Segurança da Informação em diversas formas. Por vezes, essas formas são claramente identificadas e diretas como no caso de material impresso e, nos casos indiretos, através das falas dos gerentes de segurança da informação (SOLMS, 2008). Acerca do posicionamento da Segurança da Informação na dimensão organizacional, observa-se que:

> [...] A segurança da informação é estruturada e organizada dentro da empresa. A importância desta dimensão está no fato de focar os vários tipos de melhores práticas para gestão da Segurança da Informação no qual cada estágio é vinculado a um propósito da estrutura organizacional, incluindo algum tipo de fórum sobre segurança informacional que é essencial para o bom andamento das implementações. Esta dimensão não se refere somente aos aspectos da estrutura organizacional, mas também aos aspectos da segurança da informação voltados para as responsabilidades no trabalho, a comunicação com relação às regras de segurança e ao envolvimento dos gestores com a segurança da informação (SOLMS, 2008, p.19).

Todo o movimento e o contexto corporativo que se encontra em desenvolvimento, relativo à gestão da segurança da informação, abrem perspectivas e boas oportunidades para a pesquisa no campo da Ciência da Informação. De fato, a

pesquisa a que se dá o nome de “segurança da informação” tem sido feita quase sempre relacionada ao assunto tecnologia. No presente estudo, considera-se que o fator mais importante não é a tecnologia, mas o fator humano: o usuário da informação. Este usuário da informação pode ser descrito, segundo Meadow (1992) como aquele que é fortemente dependente da informação e a utiliza com fins específicos como, por exemplo, com finalidade profissional. Essa é a visão adotada no presente trabalho, que considera que nem todo uso que se faz da informação é uso especializado e realizado por um usuário da informação. Estas pessoas que aqui se dá o nome *usuário* estão qualificadas a interpretar as informações segundo a ótica de suas respectivas áreas e, paralelamente, aptas a reconhecer e valorar esta nova informação ou fazer associações coordenadas com o que leram, agregando valor a esta informação. Várias falhas de segurança que geram grandes perdas financeiras e perda de informação sensível têm origem em pessoas, estejam elas fazendo uso ou não de sistemas automatizados.

Sendo o usuário uma fonte de informação em potencial, dotado de relevância e confiabilidade no ambiente empresarial, poderia ele ser analisado como elemento gerador de insegurança nas organizações? Em que medida estaria esse usuário da informação preparado e amparado para evitar falhas de segurança? E, mesmo estando preparado, ou seja, conhecendo os controles formais da empresa (políticas de segurança da informação, normas) e os controles informais (participando de treinamentos e dos programas de educação e conscientização), quais os aspectos peculiares ao indivíduo e seu relacionamento social que o fazem incorrer em falhas de segurança?

Essas inquietações, associadas à extrema relevância dos recursos humanos no contexto da segurança da informação demandaram esta pesquisa. A proposta é desenvolver um estudo majoritariamente quantitativo, no âmbito das Ciências Sociais Aplicadas, que venha a contribuir para esclarecer a interferência do elemento humano na segurança da informação. Busca-se identificar os perfis dos usuários que possuam inter-relação com falhas de segurança, entender com qual frequência são usados dispositivos tecnológicos que possam gerar perda de informação que tenha valor para a empresa, identificar circunstâncias nas quais as falhas de segurança ocorrem, a natureza dos incidentes de segurança e sua razão.

Para delinear a presente pesquisa, parte-se da premissa de que a efetiva gestão de segurança da informação para uma organização só é possível através de uma

abordagem sistêmico-holística. Tal abordagem diz respeito a romper com a perspectiva tecnicamente orientada e incluir em seu escopo a variedade social e as questões humanas, políticas e dos recursos organizacionais em geral (KOSKOSAS, CHARITOUDI & LOUTA, 2008).

Busca-se, assim, mudar o viés de análise em relação às pesquisas que enfatizam aspectos tecnológicos da segurança, focando na subjetividade inerente aos seres humanos, suas relações e seu comportamento informacional nas organizações. Através desta perspectiva, promover-se-á a possibilidade de analisar o tema através de visões multidirecionais e fomentar o desenvolvimento de novos panoramas para o assunto.

Desta forma, a reflexão sobre o problema, objeto da pesquisa, consta de duas etapas, cujo intuito é auxiliar as instituições nas atividades essenciais para promover a Segurança da Informação. As seguintes condições são norteadoras de tal reflexão:

Objeto de estudo: Os incidentes de segurança da informação que envolvem pessoas;

O custo/benefício envolvido na solução desse problema: ao identificar os elementos humanos que geram falhas de segurança – tais como aspectos intrínsecos à condição (personalidade) humana, o comportamento das pessoas, suas relações e condutas, para explorar como, por que e em quais circunstâncias os incidentes de segurança que envolvem pessoas ocorrem – poder-se-á reduzir custos financeiros com a perda de informações sigilosas, ganhar competitividade, além de reduzir ameaças, vulnerabilidade e riscos nas empresas. Paralelamente, haverá possibilidade de promover ações de segurança mais efetivas, uma vez que a abordagem alcança a amplitude organizacional para uma gestão de segurança da informação mais eficaz.

O **objetivo geral** do estudo**,** alinhado ao problema de pesquisa, tem a intenção de investigar a inter-relação entre o elemento humano e a segurança da informação no contexto corporativo, visando explorar as circunstâncias nas quais ocorrem incidentes de segurança da informação que envolvem pessoas. Para atingir tal objetivo geral, planejam-se os seguintes objetivos específicos.

1. Contextualizar a Segurança da Informação no âmbito da Ciência da Informação, através de levantamento teórico da área e também de outras áreas do conhecimento correlacionadas com o tema;

2. Promover um trabalho de campo para explorar como, por que e em quais circunstâncias ocorrem falhas de segurança que envolvem pessoas e entender como lidar com elas;
3. Compreender em que medida estaria o usuário da informação corporativa, preparado e amparado para evitar falhas de segurança;
4. Investigar a inter-relação entre o usuário e a segurança da informação nas organizações, para explorar elementos indicadores de falhas de segurança, com o objetivo de compreender como as organizações podem atuar frente a problemas de insegurança informacional envolvendo recursos humanos e como podem se prevenir de tais incidentes.

Destaca-se como resultados esperados:

- Determinar qual a relação dos elementos que compõem a tríade *pessoas, processos* e *tecnologia* com as ações de segurança da informação da instituição estudada;
- Promover direcionamentos para estudo de cenários na instituição estudada no que concerne à segurança da informação;
- Desenvolver possibilidades de exploração da segurança da informação frente aos cenários mais vulneráveis;
- Sugerir abordagens para processos, pessoas e tecnologias no desenvolvimento de ações de segurança;
- Enquanto campo de estudo em Ciência da Informação, este estudo se propõe a deixar como contribuição para as instituições estudadas os elementos verificadores de brechas de segurança da informação sob o aspecto humano. A partir desse estudo, as instituições poderão atuar com eficácia no desenvolvimento de ações para garantir efetividade estratégica para a segurança informacional.

Advoga-se que a Segurança da Informação, vista sob a perspectiva da abordagem sistêmica, envolve um enfoque sociocultural que permeia as relações do homem com o mundo. Doravante, a fundamentação teórica se caracteriza pela interdisciplinaridade inerente à Ciência da Informação, a qual é usada para

desenvolvimento da proposta e, a partir dessa, espera-se retratar o estado da arte em que a área se encontra.

Propõe-se então, nos capítulos 2 e 3, uma discussão acerca dos conceitos de segurança da informação, e, respectivamente a segurança da informação enquanto uma perspectiva de estudo em Ciência da Informação, de modo que se consiga o respaldo necessário para discutir o elemento humano nessa abordagem. No capítulo 3 tratar-se-á de um afunilamento das questões de segurança, debatendo a tríade pessoas, processos e tecnologia. No capítulo 4 será exposta a metodologia e o passo a passo das etapas da pesquisa. No capítulo 5 é explorada a implementação da metodologia de pesquisa e os resultados. E, por fim, no capítulo 6, serão apresentados os resultados, e, a uma discussão sobre eles, para na sequência, no capítulo 7, descrever as considerações finais.

2 Visão preliminar sobre a Segurança da Informação: Definições e abrangência da Segurança da Informação

Muitas pesquisas focando a Segurança da Informação abordam o tema no viés tecnológico. Entretanto, parecem existir poucos estudos sobre Gestão de Segurança da Informação que se concretizam na área da Ciência da Informação. A intenção desta pesquisa é utilizar da perspectiva da Ciência da Informação, enquanto área interdisciplinar, para desenvolver um estudo cujo olhar esteja no âmbito social da Segurança da Informação.

Através do predicado interdisciplinar da Ciência da Informação, principalmente focando sua propriedade no que concerne à organização e uso da informação, aponta-se que o universo da informação estruturada e registrada como domínio da Ciência da Informação utilizado nessa pesquisa. Entende-se, preliminarmente, a informação como um ativo da organização, utilizado para compor o valor da empresa, sendo dever desta organização atuar em sua proteção.

As empresas lidam com um fluxo constante de informações e têm à sua disposição toda uma gama de ferramentas, técnicas e procedimentos advindos das pesquisas em Ciência da Informação, bem como o suporte tecnológico provido pela Tecnologia da Informação para efetuar a gestão de suas informações.

O avanço tecnológico tem proporcionado o processamento de um grande volume de informações armazenadas em meio digital e, com a tecnologia das redes, uma nova gama de problemas surgiu, uma vez que a organização saiu dos limites geográficos da empresa. Ataques virtuais, contaminação por vírus, adulteração de dados, acessos indevidos aos sistemas de informação etc., são fatores que conferem a necessidade de proteção da informação, através de um programa estratégico de segurança da informação.

Lacey (2009) já observava essa transição dos limites organizacionais quando assinalou que as empresas precisam mudar o foco das necessidades de segurança, passando de uma perspectiva interna - voltada exclusivamente para as necessidades de segurança dentro da empresa, e adotando um olhar que acompanhe o progressivo deslocamento das necessidades de segurança para fora dos limites da empresa.

A era das empresas globais, virtuais e conectadas arrebata o mundo, sendo que nesta a geografia não é mais barreira, e traz consigo muitas oportunidades e riscos em contrapartida. Esses riscos envolvidos no processamento de informações e nas transações comerciais geram vulnerabilidades e ameaças, cujos entraves precisam ser sanados para o sucesso da organização.

Almeida (2010) coloca que, na tentativa de lidar com as questões de segurança da informação, as empresas focam seus esforços nos mecanismos de proteção baseados em políticas de segurança da informação, análise de riscos e classificação da informação:

> Uma política de segurança é um plano de alto nível que estabelece como a segurança deve ser praticada e em que nível de segurança – com custos e benefícios inerentes – a organização está disposta a aceitar.
>
> A análise de riscos consiste na prática de confrontar o valor da informação com os riscos inerentes às perdas, bem como identificar meios de proteção para reduzir riscos.
>
> Os procedimentos de classificação da informação agrupam entidades similares em categorias, possibilitando implementar medidas de proteção com vistas à garantia da confidencialidade da informação (Almeida, 2010, p.156).

No universo empresarial, a concepção acerca do que vem a ser segurança vem evoluindo e não mais se restringindo apenas à questão técnica. A perspectiva da Segurança da Informação focada nos negócios ganha espaço, ratificada pelas necessidades da sociedade.

O fato da segurança da informação ser uma necessidade do negócio é destacado por Almeida (2010), que ainda coloca que, apesar dessa ratificação, muitas organizações não conseguem alavancar ações de segurança informacional, haja vista que projetos e recursos necessários são caros e inviabilizam as atuações.

Em contrapartida, observa-se, conforme pontuado por Wylder (2004), que muitas organizações ainda não têm se comprometido com o desenvolvimento de um programa de segurança de informações completo, pelo fato de ainda não terem integrado os programas de segurança informacional à totalidade dos negócios. Concomitantemente, percebe-se que algumas empresas buscam formas de estruturar adequadamente a comunicação para segurança e, em alguns casos, tratam a segurança informacional como funções estritamente tecnológicas ou de controle. Para finalizar, o autor compara a área de segurança da informação com as áreas de auditoria e finanças,

expondo que todas as inquietações sociais e formas diferentes de se tentar delinear um escopo para a segurança da informação são características peculiares de uma área que ainda está evoluindo, quando comparada com outras que já estão solidificadas.

Em meio à constante evolução e à própria dinâmica do mercado, as demandas empresariais se estruturam na necessidade de descobrir soluções estratégicas para seus negócios. Observa-se que a segurança da informação é uma demanda social, dotada de relevância na economia globalizada, como um dos elementos garantidores de competitividade. Por isso é importante que os empresários busquem atrelar ao negócio da empresa as variáveis *segurança* e *proteção dos ativos informacionais* como elementos integradores do negócio principal, uma vez que proteção às informações é fundamental para o sucesso e sobrevivência no mundo de hoje.

Logicamente, a proteção dos dados não se limita apenas aos ativos tecnológicos, haja vista que a empresa não possui dados apenas em formato digital. A empresa possui informação disponível e relevante ao negócio em outras fontes, inclusive externas à organização, como governos, conselhos de classe, fornecedores etc., além do fato da segurança informacional envolver outros aspectos como as questões políticas, culturais e de natureza física (ALMEIDA, 2010). O autor conclui dizendo:

> Problemas na implementação de estratégias de segurança da informação começam pela dificuldade em definir o que deve ser protegido, qual nível de proteção necessário e quais ferramentas devem ser utilizadas no ambiente corporativo. Cabe ainda à organização descobrir em que contexto se manifesta a informação relevante para seus objetivos de negócio, bem como as necessidades corporativas em relação à segurança. Essas necessidades são influenciadas por fatores humanos e por fatores inerentes ao próprio ciclo de vida da informação (Almeida, 2010, p.155 e 156).

Por isso, com relação à proteção dos ativos informacionais, vale esclarecer que esses ativos, segundo Lacey (2009), não incluem apenas informações valiosas que se encontram nas bases de dados e documentos da empresa, ou em suas marcas e reputação, mas também o valor fornecido pelo *know-how*, habilidades e relacionamentos que são incorporados em redes da organização, tanto dentro como fora de seus limites corporativos.

Quando se trata de ativos informacionais, é interessante pensar a perspectiva de um uso responsável da informação para uma sociedade mais segura. Entretanto, no âmbito organizacional, para que esta suma se torne real, é preciso pensar que a segurança começa na cultura da empresa, através do desenvolvimento de ideias acerca

da proteção da informação e da responsabilidade de cada colaborador nesse processo (WYLDER, 2004).

Ao unir as perspectivas abordadas pelos autores, tem-se que a segurança da informação deve abranger a tríade tecnologia, processos e pessoas, uma vez que esses elementos coexistem no contexto organizacional (SVEEN, TORRES & SARIEGI, 2009).

A proposta recomendada da tríade traz a reflexão de que a união das abordagens pertinentes a cada elemento forme uma visão totalizadora. O imperativo desta abordagem é simples e completo e acredita-se ser esta a base para se desenvolver um programa estratégico de segurança da informação, uma vez que o contexto empresarial será compreendido à luz de três olhares – as pessoas como elementos formadores da cultura e do contexto organizacional, os processos como veículos informacionais e as tecnologias como ferramentas que sustentam os processos e as necessidades informacionais das pessoas. Através do detalhamento das propriedades pertinentes a cada elemento - pessoas, processos e tecnologia - e sequente união destas variáveis na esfera empresarial, acredita-se obter um arcabouço para desenvolvimento das ações de um programa estratégico de segurança informacional.

A amplitude de um programa de segurança da informação deve contemplar ainda outros quesitos que foram discriminados por Lacey (2009), sobre a necessidade de desenvolver novos modelos de avaliação, exploração e manutenção dos ativos informacionais das companhias, e também identificar esses ativos e reconhecer seu valor para protegê-los. Paralelamente, é importante conhecer minuciosamente o negócio da empresa e os riscos vinculados, para desenvolver estratégias de segurança informacional, uma vez que estas organizações passaram a trabalhar em um mercado global, interconectado e que pleiteia exercer poder através do domínio da informação.

Entendendo que o caminho para uma solução de segurança informacional nas empresas seja o desenvolvimento e instituição de um programa estratégico, e diante da impossibilidade de se estudar a fundo todos os elementos que compõem a tríade – pessoas, processos e tecnologia –, que são a base, conforme dito anteriormente, do referido programa, este estudo focará o elemento *pessoas*. A opção por estudar as pessoas no que concerne à segurança da informação vem da constatação de Lacey (2009), ao afirmar que a tecnologia é essencial para a segurança, contudo, esta tecnologia é projetada, ou seja, implementada e operada por pessoas. Assim, é o fator

humano que determina as formas como usamos os sistemas de informação ou o uso indevido destes. São as pessoas que gerem a segurança física e concedem acesso aos sistemas. São as pessoas que também causam, relatam e gerenciam a resposta das empresas frente a casos de violação e incidentes de segurança.

Desta forma, ao analisar o contexto da segurança informacional, observou-se que o elo *pessoas* da tríade pode ser a aresta dissonante e pouco explorada nas organizações ao desenvolver soluções de segurança informacional.

A proposta é que, na sequencia, sejam analisadas as definições sobre segurança da informação, para entender como a concepção do termo pode interferir no entendimento das pessoas acerca de suas ações no que concerne à segurança informacional, na compreensão das pessoas com relação a suas contribuições para garantir um bom andamento das ações propostas no programa de segurança da informação e, finalmente, sua própria inserção como agente consolidador do programa de segurança da informação.

Dessa forma, o dinamismo do mercado traz consigo a competitividade, demandando das empresas especial atenção na proteção de seus ativos, para evitar que seus diferenciais competitivos sejam perdidos para os concorrentes.

Muitos estudos com foco na proteção dos ativos informacionais das empresas foram efetuados, sendo vários realizados por pesquisadores da área de processamento de dados e de telemática (SIANES, 2006). Complementando esta análise, Sianes relata que:

> Essa situação trouxe conseqüências [*sic*] interessantes. Esses profissionais dominaram esse campo de atuação e impuseram um enfoque voltado diretamente para as informações armazenadas em sistemas de informação, notadamente informatizados. Assim, metodologias, técnicas e práticas de segurança da informação são desenvolvidas prioritariamente para computadores, ignorando ou menosprezando outras formas de registro ou generalizando de modo inadequado suas conclusões e estudos para outros tipos de suportes e formas de representação. (SIANES, 2006, p.136)

Percebe-se, através da análise de alguns estudos sobre segurança da informação (KRAUS, 1980; GAO, 1988; GARFINKEL **&** SPAFFORD, 1996; ISACF, 2000; ISSEA, 2003), WOOD, et al 1987; CIAO, 2000, OECD, 1992; WOOD, et al 1990; NIST/CSD, 1998, NEUMANN e PARKER, 1989; MEADOWS,1992; LEVINE, 1995; HOWARD **&** LONGSTAFF, 1998), o porquê do viés tecnológico da segurança da

informação ter ganhado tanta força e ter sido mais amplamente desenvolvido, pelo menos até o momento, que os outros pilares que compõem a segurança da informação.

Segundo Wylder (2004) há uma tendência de que as organizações priorizem os domínios cuja abordagem seja técnica ou que implementem parte da composição do domínio do programa de segurança da informação. Entretanto, essa priorização precisa ser mudada, uma vez que considera soluções momentâneas para problemas específicos sem se inteirar e abordar todos os elementos envolvidos nas questões de segurança informacional. É imperativo na sociedade da informação e nas organizações modernas proteger seus recursos informacionais em sua totalidade.

Analogamente, outro ponto que merece destaque ao analisar a evolução das percepções da sociedade acerca da Segurança da Informação, se refere aos episódios de segurança que caracterizaram as décadas. Esta perspectiva é retratada por Lacey (2009) quando ele observa que cada década tem trazido um novo enfoque à segurança, através da progressiva extensão das redes.

> A década de 1970 introduziu a avaliação de risco. A década de 1980 incentivou unidades de negócio para estabelecer centros de dados seguros. A década de 1990 mudou o foco de segurança para redes corporativas. Nos primeiros anos do século 21 foi introduzido o comércio eletrônico (LACEY, 2009, p.32, tradução própria) [1].

É interessante pensar em um paralelo no sentido de refletir comparativamente como a evolução das tecnologias é que propiciam a evolução nos enfoques dados à segurança da informação, assim como na Ciência da Informação, quando as tecnologias mudaram a percepção acerca da informação no contexto da sociedade e as tecnologias da informação e da comunicação surgiram e dominaram um contexto econômico, político e social, de modo a transformar todo um modo de vida da sociedade, que posteriormente veio a se chamar *sociedade da informação.*

Ghernaouti-Helie (2009) traz uma reflexão congruente às postuladas acima, uma vez que a autora propõe que proteção à informação é quesito proeminente na sociedade da informação. A autora coloca que, independente do nome que seja dado à "segurança da informação", tais como *segurança digital* ou *segurança das tecnologias da informação*, esta percepção reflete as necessidades da sociedade de entender os

[1] The 1970s introduced risk assessment. The 1980s encouraged business units to establish secure datacentres. The 1990s moved the focus of security to enterprise networks. The early years of the 21st century introduced electronic commerce.

riscos vinculados ao uso das Tecnologias da Informação e da Comunicação (TIC) no nosso dia-a-dia. Assim, entender os riscos inerentes ao uso das tecnologias é, também, adotar ações para minimizar riscos e percebê-los através de um nível aceitável de controle.

Essas abordagens e reflexões são interessantes porque se consegue entender o papel fundamental da tecnologia, como agente transformador dos processos e a evolução de áreas como a Segurança da Informação, mediante as mudanças e inovações tecnológicas e as novas demandas da sociedade. Todas essas questões e abordagens dadas à Segurança da Informação merecem agora especial reflexão, principalmente por que a demanda da sociedade é por soluções que integrem e interajam com todo o contexto organizacional. Desta forma é necessário, conforme apontado por Wylder (2004), se mudar para uma posição mais madura, pois a segurança deve ser integrada como parte do próprio negócio e, ao fazer isso, programas de segurança da informação precisam se deslocar de implementações táticas de tecnologia para parceiros estratégicos nos negócios.

Essa nova perspectiva, de ver a segurança da informação como agente parte dos negócios da empresa, requer desta um entendimento que explicite seu objetivo no ambiente corporativo.

Efetivamente, versar sobre a definição de segurança da informação é primordial para seu entendimento, uma vez que, conforme pontuado por Marciano (2006), muitos conceitos são apresentados acerca do que a segurança da informação faz, mas não do que ela efetivamente significa.

Ghernaouti-Helie (2009) expõe que o termo “Segurança da Informação” pode ter vários significados, dependendo do enfoque que é dado e do contexto no qual é empregado. Desta forma, o conceito pode estar vinculado à espionagem, ao terrorismo, à criminalidade, à manipulação de conteúdos não permitidos ou ilícitos, à vigilância computacional, ao controle excessivo ou à necessidade de lutar pelo respeito aos direitos humanos fundamentais, tais como a privacidade.

Ao se investigar sobre o tema da informação junto aos autores da área, observa-se um ponto em comum – o olhar para a informação como um recurso que requer proteção. Nesse sentido, algumas reflexões foram extraídas e trazidas para este estudo, haja vista a necessidade de se encontrar abordagens que considerem a interação

entre as variáveis pessoas, processos e tecnologia, de modo que se atenda à demanda das empresas de proteger seus ativos informacionais de forma totalizadora.

Para iniciar, trar-se-á reflexão de Wylder (2004), cuja proposta é que a segurança da informação seja definida nos parâmetros de um programa de segurança informacional, cujo plano é o de reduzir riscos associados ao processamento de informações. O autor ainda coloca que os conceitos básicos de segurança envolvem os elementos:

- Confidencialidade: A prevenção do uso ou divulgação não autorizada de determinada informação;
- Integridade: Garantir que as informações sejam precisas, completas, e que não foram modificadas por usuários não autorizados ou processos;
- Disponibilidade: Garantir que os usuários tenham acesso rápido e confiável aos ativos de informação.

A proposta do autor cita a necessidade de um programa de segurança informacional, contemplando todos os níveis da organização, haja vista que o processamento de informações ocorre em toda a estrutura da empresa e envolve tanto elementos técnicos e processuais quanto humanos da composição organizacional.

Sobre os elementos que compõem a estrutura da empresa, Marciano (2006) dá especial ênfase ao fator humano da composição organizacional. Segundo, ele a segurança da informação é:

> Um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso (Marciano, 2006, p.114).

Essa perspectiva de discussão acerca da segurança da informação e dos elementos que a compõem, nos mostra como o autor enfatiza, em seu estudo, aspectos relativos às interações sociais dos indivíduos, os sistemas de informação e o uso da informação de acordo com as etapas de seu ciclo de vida.

Ghernaouti-Helie (2009) contribui ao versar sobre as questões que envolvem a segurança da informação sugerindo que estas podem ser discutidas no âmbito da dimensão estratégica das Tecnologias da informação e da comunicação, da infraestrutura e serviços para o estado, da organização, competitividade e segurança das pessoas. Assim, a segurança da informação tem como perspectiva a possibilidade de ser estudada no âmbito interdisciplinar e de multi-interesses, colocando os indivíduos no centro das questões de segurança vinculadas às TIC, e associando esta a um elemento colaborativo e necessário no processo de desenvolvimento de uma sociedade da informação consciente e inclusiva.

Complementar a esta proposta é a reflexão de Sveen, Torres **&** Sarriegi (2009) quando colocam que a segurança da informação pode ser tratada como um processo global de melhoria da qualidade. Os investimentos em controles técnicos devem ser equilibrados com investimentos formais e informais, com especial atenção ao processo de criação de conhecimento.

Os pontos de destaque desta abordagem são a do aprendizado organizacional ou criação de conhecimento e a melhoria da qualidade, uma vez que, no primeiro caso, as empresas estão incentivando esta prática e, no segundo caso, o ato de melhoria na qualidade indiretamente agrega valor nos ativos da organização, sendo, em ambos os casos, que o objetivo das empresas é garantir a competitividade e auferir lucros maiores.

Já os autores Vroom **&** Solms (2004), ao fazer uma leitura das normas internacionais sobre segurança da informação, dando ênfase nas políticas de informação, retratam que a segurança da informação é tida como os processos e procedimentos que o empregado cumpre, a fim de proteger a confidencialidade, integridade e disponibilidade das informações e outros bens valiosos da empresa. Apesar da visão dos autores abordar o conceito de segurança da informação focado em ações de política informacional, vale salientar como ponto de destaque a proteção aos ativos, inclusive hardware e software, através dos elementos confidencialidade, integridade e disponibilidade que são tidos como requisitos em ações de segurança.

Outra definição acerca da segurança da informação é apontada pelo Governo Federal do Brasil, na qual:

> Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a

> modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (GOVERNO FEDERAL DO BRASIL, 2000)

Essa abordagem do governo brasileiro traz uma visão integrada de vários elementos combinados que são parte do contexto organizacional, incluindo a proteção aos ativos tácitos – recursos humanos – e os explícitos – documentação virtual ou material. Tão relevante quanto a proteção dos ativos é o desenvolvimento e implementação de ações para detectar, deter, prevenir e documentar ameaças, mostrando um conceito atemporal, uma vez que vincula presente, passado e futuro ao analisar potenciais riscos, ameaças e vulnerabilidades. Acredita-se que a expectativa da sociedade seja exatamente a de conseguir integrar a totalidade das variáveis para delas extrair os ativos passíveis de proteção.

A última definição extraída para este estudo é a da ISO/IEC 1799:2005, cuja abrangência é dividida em dois momentos que se integram. O primeiro diz que:

> A segurança da informação é a proteção de informações de uma ampla gama de ameaças para garantir a continuidade dos negócios, minimizar os riscos dos negócios e maximizar o retorno sobre investimentos e oportunidades de negócios. (ISO/IEC 1799:2005)

Já o segundo momento propõe uma abordagem complementar ao primeiro e reza que:

> A segurança da informação é conseguida através da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, onde for necessário, para assegurar que a segurança e os objetivos específicos dos negócios da organização sejam alcançados. Isto deve ser feito em conjunto com outros processos de gerenciamento de negócios. (ISO/IEC 1799:2005)

Esta abordagem ratifica um aspecto importante que é o fato de se tratar a segurança da informação como parte dos negócios de uma empresa, cujos fatores chave são: maximizar o retorno aos investimentos feitos e as oportunidades de negócios e minimizar os riscos.

Como se pode observar a partir das definições apresentadas até aqui, são múltiplas as perspectivas adotadas pelos autores para definir a Segurança da Informação.

Mudar a perspectiva de análise e passar a tratar a Segurança da Informação através de uma perspectiva sistêmico-holística vem ao encontro com as propostas desta pesquisa, uma vez que a segurança é um problema multifacetado cujas variáveis interagem em um único ambiente e demandam confidencialidade, integridade e disponibilidade frente aos riscos, ameaças e vulnerabilidades.

Esta perspectiva não permite eleger uma definição de Segurança da Informação para nortear este estudo, haja vista que as abordagens abrigam aspectos distintos, mas totalmente relevantes. A solução vislumbrada é a de se trabalhar com todas as abordagens analisando sua contribuição e inferência em cada caso. Assim, pretende-se estabelecer um uso adequado de cada conceito de segurança frente a cada situação.

Acredita-se que a Segurança da Informação deva ser tratada no âmbito da totalidade dos elementos que envolvem o assunto e de forma interativa e integrativa aos negócios. A proposta de Wylder (2004) é que se desenvolva um programa estratégico de segurança informacional focado nos seguintes elementos:

- Visão da empresa;
- Busca de uma melhoria em seus processos;
- Garantia de competitividade e qualidade;
- Aprendizado organizacional;
- Geração de conhecimento;
- Gestão de organização e uso das informações;
- Interações sociais;
- Proteção à confidencialidade, integridade e disponibilidade dos ativos organizacionais, sejam eles tácitos ou explícitos;
- Maximização do retorno de investimento e das oportunidades de negócios;
- Proteção, inclusive de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo, sejam estas internas e/ou externas à organização;

- Detecção, detenção, prevenção e documentação, vinculando presente, passado e futuro, ao analisar potenciais riscos, ameaças e vulnerabilidades aos ativos empresariais.

Ao unir esses elementos na perspectiva organizacional, observa-se que uma correta modelagem do negócio da organização, somados a um planejamento estratégico e a uma gestão eficiente, à busca por organização dos processos corporativos, inovação, segurança da informação e foco na gestão das informações e do conhecimento empresarial podem ser possíveis arenas nas quais as empresas podem se sustentar para desenvolver sua competitividade no mercado.

Doravante, usar-se-á tanto a perspectiva analítica demonstrada acima quanto os parâmetros do programa estratégico de segurança informacional como direcionadores dos trabalhos. Apesar de não haver possibilidade de se explorar e validar todos os elementos do programa estratégico de segurança informacional na metodologia de pesquisa, uma vez que algumas variáveis, como por exemplo, a maximização do retorno de investimentos e das oportunidades de negócios demande um tempo maior de observação e análise, tempo este indisponível na pesquisa de mestrado. Não obstante, há expectativa de que as empresas incluam todos os parâmetros de programa estratégico de segurança informacional, assim como os elementos da perspectiva analítica em seu escopo de desenvolvimento de um programa de segurança da informação.

Ressalta-se que essa seção contribui na construção do instrumento de coleta de dados no que concerne à necessidade de explicitar que a abrangência da Segurança da Informação deve ser gerida através de uma perspectiva sistêmica e que sua conceituação deve igualmente contemplar todos esses atores que interferem ou sofrem interferência da segurança ou insegurança dos ativos informacionais.

3 Segurança da Informação: Perspectivas de estudos em Ciência da Informação

A Ciência da Informação enquanto área pode ter sua história segmentada em vários elementos constitutivos que reiteram sua grandeza. As subáreas - Gestão da Informação e do Conhecimento e Organização e Uso da Informação serão os campos no quais será explorado o tema Segurança da Informação e sua contribuição na atual era da Informação e do Conhecimento.

A Gestão da Informação e do Conhecimento é uma das subáreas escolhidas, haja vista que se implementar a gestão estratégica da segurança informacional corporativa requer que elementos como gestão das informações para proteger os ativos, aprendizagem organizacional, compartilhamento e troca de conhecimento sejam ações factíveis de serem executadas pela organização que vê a informação como ativo de valor e gerador de competitividade.

Nessa mesma vertente a linha de Organização e Uso da Informação contribui com essa perspectiva delimitando as formas para se organizar e limitar quais informações podem ser destacadas como ativos de valor para serem geridas através da gestão da informação e consequentemente quais ativos devem ser protegidos na gestão estratégica de segurança da informação.

Antes de se tratar das subáreas da Ciência da Informação, faz-se importante contextualizar a própria Ciência da Informação enquanto arena que ampara os estudos em segurança da informação.

Os problemas cotidianos para os quais se busca solução, inclusive aqueles oriundos de necessidade de segurança informacional, surgem da vivência em sociedade. A inter-relação entre vida cotidiana e realidade é trazida por Berger **&** Luckmann (1994) que afirmam que a vida cotidiana é um mundo que se origina no pensamento e na ação de homens comuns, sendo afirmado como real por eles. A Ciência da Informação, como uma Ciência Social, procura conhecer essa realidade e, para tanto, busca definir problemas suscetíveis de resolução através da pesquisa científica (Silva e Pinto, 2001).

> Apreendo a realidade da vida diária como uma realidade ordenada. Seus fenômenos acham-se previamente dispostos em padrões que parecem ser independentes da apreensão que deles tenho [...]. A realidade da vida cotidiana aparece já objetivada, isto é, constituída

> por uma ordem de objetos que foram designados como objetos antes de minha entrada em cena. A linguagem usada na vida cotidiana fornece-me continuamente as necessárias objetivações e determina a ordem em que estas adquirem sentido e na qual a vida cotidiana ganha sentido para mim (BERGER **&** LUCKMANN, 1999, p.38).

Nesta mesma linha de reflexão, os autores Silva e Pinto (2001) colocam que conhecer a realidade é construir instrumentos que gerem informação sobre esta realidade e modos de torná-la inteligível sem se confundir com ela.

No século XXI vive-se uma realidade na qual todos os cidadãos vivem à mercê de ter seus dados pessoais ou de suas corporações roubados, dados estes que são processados no ambiente corporativo, com o objetivo de gerar vantagem competitiva e manter a empresa viva no mercado. Portanto, criar uma solução que promova mais segurança aos ativos informacionais de cidadãos e empresas é entendida como uma demanda da sociedade.

Como a Ciência da Informação se enquadra como uma Ciência Social, visto que investiga parte da realidade da sociedade e esta parte constitui seu objeto de estudo, observa-se que ocorre um direcionamento que sai da realidade e foca no sujeito (RENDÓN, 2008). Diante da prerrogativa que o foco de estudos seja o sujeito é necessário entender, conforme pontuado pelos autores Silva **&** Pinto (2001, p.17), que todo comportamento só é compreensível dentro de uma totalidade, ou seja, recursos, representações, ações e instituições sociais intervêm nas mais elementares relações entre pessoas.

Desta forma, a autora Gomez (2000), relata que a constituição de um domínio da Ciência da Informação seria a instauração de um ponto de vista que recorre à ampla zona transdisciplinar, com dimensões físicas, comunicacionais, cognitivas e sociais ou antropológicas. Nesse contexto, a mesma autora atribui como objeto da Ciência da Informação um conjunto de regras e relações tecidas entre agentes, processos e produções simbólicas e materiais (GOMEZ, 2000, p.121).

A perspectiva de objeto adotada por Gomez (2000), supracitada, é mais ampla quando comparada com os autores citados a seguir, uma vez que Rendón (2008) postula como objeto da Ciência da Informação o sistema informativo documental formado pela interação entre informação, documento, usuário e instituição informativa documental e, para Pinheiro (2004) o objeto da Ciência da Informação é a informação. Sendo que, para esta autora, o termo informação não pode ser definido nem medido e, por este motivo aplica-se no campo da Ciência da Informação a configuração de fenômeno de geração,

comunicação e uso da informação. Uma consideração importante exposta por Pinheiro (2004) relata que muitos campos do conhecimento utilizam-se da informação, mas poucos são aqueles que a tornam seu objeto de estudo, como é o caso da Ciência da Informação.

Outra reflexão importante que corrobora com este estudo é a de Pinheiro **&** Loureiro (1995) quando analisam afirmações de Wersig e propõem que a Ciência da Informação não deve ser pensada nas diretrizes da ciência clássica e sim em termos de uma nova ciência, cuja pesquisa não se dirige, preliminarmente, para um desvendamento do mundo e sim para solução ou trato de problemas.

Fazendo uma análise sucinta desta perspectiva, observa-se que uma das características da Sociedade da Informação é o encurtamento das distâncias geográficas, promovido pelo desenvolvimento das tecnologias da informação e da comunicação, ou seja, para a sociedade a distância geográfica era um problema que foi resolvido, ou parcialmente resolvido, com o desenvolvimento e uso das tecnologias da informação e da comunicação. Ao se aplicar outros exemplos de necessidades da Sociedade da Informação vê-se que a maior parte deles, para não dizer todos, estão voltados para a solução ou trato de problemas. Ou seja, todas essas ocorrências e vários outros elementos ratificam a proposta de Wersig de tratar a Ciência da Informação como uma ciência nova, focada em soluções ou tratamento de problemas da sociedade.

Pinheiro **&** Loureiro (1995), ao analisar Wersig, assinalam que:

> [...] um dos principais problemas no estudo da ciência da informação é seu fracionamento em inúmeras disciplinas, obrigando o cientista a lidar com dados fragmentados de natureza empírica e teórica. Prossegue, afirmando que, "se a ciência da informação existe, qualquer que seja a denominação dada a esse campo, ela não possuirá uma teoria, mas uma estrutura proveniente de um amplo conceito científico ou modelos e conceitos reformulados. Esses serão intertecidos a partir de seu desenvolvimento e do problema do uso do conhecimento nas condições pós-modernas de informatização. Havendo uma interconexão entre tudo, a ciência da informação deve desenvolver um sistema de navegação conceitual". (PINHEIRO **&** LOUREIRO, 1995, p.4-5)

A perspectiva apresentada por Dupas (2001, p.70) contribui com esta linha de pensamento quando ele diz que a ciência da contemporaneidade aspira por utilidade, pretendendo ser o aspecto teórico de uma perspectiva do ser, cujo aspecto prático se expressa pela tecnologia. O mesmo autor ainda pontua que o papel do filósofo da informação é o de reduzir ambiguidades no mundo cotidiano apoiando-se na tecnologia e de entender o ser racionalmente, ou seja, dar um sentido racional ao ser. Nessa

perspectiva o autor define racionalizar como o ato de submeter o processo à técnica e desse modo livrá-lo de seus excessos (irracionalidades) (DUPAS, 2001, p.71).

Fazendo um apanhado e finalizando a análise a partir das considerações dos autores pontuados acima, acredita-se que pensar a ciência da Informação em termos de uma ciência nova seja o caminho. Partindo do conceito de que ciência é caracterizada como uma representação intelectualmente construída da realidade (SILVA & PINTO, 2001, p.11), há a necessidade de desenvolver novos parâmetros e diretrizes de avaliação, de análise e de constituição. Independente dos critérios científicos de avaliação da Ciência da Informação, um ponto em comum se sobressai - a perspectiva de orientação por problemas. E, diante da necessidade de se buscar soluções e explicações para fenômenos em determinado contexto sócio-histórico e espaço-temporal, Harold Borko, em 1968, propõe a seguinte definição para a Ciência da Informação (CAPURRO, 1985; SARACEVIC,1996):

> "Ciência da Informação é a disciplina que investiga as propriedades e o comportamento da informação, as forças que governam o fluxo de informações e os meios de processar a informação para otimizar sua acessibilidade e usabilidade. Interessa-se pelo corpo de conhecimentos relacionados à criação, coleta, organização, armazenamento, recuperação, interpretação, transmissão, transformação e utilização da informação. [...] Tem tanto um componente de ciência pura, que investiga a essência do assunto sem considerar sua aplicação, quanto um componente de ciência aplicada, que desenvolve serviços e produtos [...] (BORKO, 1968).

À medida que a sociedade demanda por respostas os questionamentos evoluem e, aquele conhecimento, resultado de uma pesquisa, que antes foi suficiente para se entender determinado fenômeno da realidade, agora volta a ser questionado, em um novo contexto, representando um processo continuado e sempre incompleto. Além da dinamicidade incorporada nas necessidades da sociedade no que se refere principalmente à informação, vale resgatar a fala de Dupas (2001) que incorpora ao conceito de ciência da contemporaneidade o elemento utilidade. Portanto, diante da necessidade da ciência de ser, nos dias atuais, útil às questões da sociedade, e, do crescimento das tecnologias promovido por uma demanda social por informação de forma rápida, é que Saracevic (1996) propõe a seguinte definição da Ciência da Informação contemporânea:

> "A Ciência da Informação é um campo dedicado às questões científicas e à prática profissional voltadas para os problemas da efetiva comunicação do conhecimento e de seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e

> das necessidades de informação. No tratamento destas questões são consideradas de particular interesse as vantagens das modernas tecnologias informacionais." (SARACEVIC, 1996, p.47)

Na medida em que se busca entender os questionamentos e encontrar soluções para os mesmos, observa-se que os problemas estudados não são passíveis de serem resolvidos no âmbito de uma única disciplina. Assim, a Ciência da Informação é influenciada por diversas áreas do conhecimento, ratificando sua característica interdisciplinar.

Essa característica interdisciplinar faz com a Ciência da Informação se aproprie, por exemplo, dos contextos sócio-corporativos, amplamente estudados pela Administração, para neles estudar a informação.

Assim nesse segundo momento, dedica-se espaço para estudar exploratoriamente as subáreas da Ciência da Informação.

O termo gestão surgiu, segundo Braverman (1977), da necessidade de gerenciar o trabalho humano, desde a construção das pirâmides egípcias à muralha da China, abrangendo vários outros capítulos da história da humanidade. No entanto, é com o surgimento do capitalismo industrial que a figura do gerente emerge tal como é conhecida na atualidade. Se antes a construção de determinadas obras era realizada para exaltar os faraós ou para fins militares e civis, no capitalismo o uso coordenado da mão-de-obra tem o objetivo da geração de lucro.

Um dos primeiros autores a tratar do trabalho gerencial foi Taylor, em seu livro Princípios de Administração Científica, no qual relata o trabalho gerencial e aquilo que compete aos trabalhadores e à administração das empresas. Nessa mesma temática, Fayol complementa que as diversas atividades de uma empresa devem ser classificadas e separadas por função: técnica, comercial, financeira, de segurança, de contabilidade e administrativa.

Essa visão preliminar é importante no sentido de contextualizar o leitor de que a consolidação da administração e da gestão dos meios de produção e do trabalho humano foi uma das etapas evolutivas para que se chegasse na gestão da informação e do conhecimento e consequentemente na organização e uso adequado das informações do ambiente empresarial.

Dessa forma, ressalta-se que as transformações advindas da Revolução Industrial foram as mais radicais já registradas em documentos escritos. O desenvolvimento da indústria e dos meios de produção era crescente, principalmente pelo fato de serem

dirigidos pela perspectiva do lucro. O aumento da necessidade de controle em virtude das tarefas complexas e requisitos operacionais caracterizaram a crescente burocracia estatal e as empresas de grande escala no final do século XIX. A necessidade estatal de intervir na vida social e econômica gerou nas empresas a obrigação de planejar a produção, monitorar mercados, auditar etc., e, para esta tarefa contaram com o uso, a partir do final do século XIX e início do XX, das técnicas e tecnologias da informação. A autora Black (2006), ratifica este ponto de vista através da citação abaixo:

> Uma variedade de métodos inovadores apareceu para melhorar a informação das organizações e infraestruturas de comunicação: análise estatística, representação gráfica, a memória interna, revistas para o *staff*, reuniões de gestão, os sistemas de classificação de documentos, o manual de procedimentos e protocolos escritos. Estes, por sua vez, eram apoiados por uma série de "dispositivos" inovadores: duplicadores de estêncil, máquinas de escrever, telefones, máquinas de contabilidade, armários, e um cartão de índices, e posteriormente surgiram a máquina de cartões perfurados, microfilmes, e fotostática (BLACK, 2006, p. 452).

A evolução das tecnologias da informação e da comunicação (TIC´s) propiciou uma explosão ao acesso à informação e, consequentemente, multiplicaram na sociedade o interesse pelas informações e as formas como esta é obtida, organizada e disseminada. Este interesse da sociedade pela informação promoveu à mesma a uma categoria de ativo, ou seja, algo que possui valor e gera ganhos. Como a informação adquiriu caráter de elemento estratégico para a sociedade, seu nome mudou para Sociedade da Informação.

As autoras Legey **&** Albagli (2000) relatam que a sociedade da informação decorre de mudanças distintas da vida humana em sociedade, as quais interagem em sinergia e confluem para projetar a informação nas esferas sóciopolítica e econômica.

> "A expressão Sociedade da Informação, refere-se a um modo de desenvolvimento social e econômico, em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação desempenham um papel central na atividade econômica, na geração de novos conhecimentos, na criação de riqueza, na definição da qualidade de vida e satisfação das necessidades dos cidadãos e de suas práticas culturais (LEGEY **&** ALBAGLI, 2000, p.1).

Nota-se que realmente houve mudanças no estilo de vida da sociedade. No caso corporativo, observa-se que o desenvolvimento das tecnologias propiciou a centralização das atividades burocráticas nos escritórios, nos quais, para maior

velocidade, os métodos de trabalho e as formas de documentação foram padronizados para que se viabilizasse o investimento em máquinas de escritório.

Avaliando a manifestação da tecnologia na sociedade para o processamento da informação, Dupas (2001) afirma que os custos sociais gerados pela mudança nos padrões tecnológicos aparecem como inevitáveis. A divisão social do trabalho subverte-se pela contínua evolução dos sistemas técnicos, motivada pelo embate da concorrência.

O dinamismo trazido com o desenvolvimento das tecnologias gerou na sociedade uma demanda por informação de forma rápida e que atenda a seus objetivos cotidianos de forma eficiente e eficaz.

Nessa perspectiva observou-se uma crescente utilização de técnicas de transmissão, armazenamento de dados e informações a baixo custo, além das inovações organizacionais, sociais e legais, alavancando inovações produtivas, técnicas, organizacionais e comunicacionais sentidas em todos os níveis da sociedade.

A crise ocorrida em 1929 abriu caminho para que o Estado se tornasse um ator econômico direto. Ele assume o papel de mobilizar capitais para investimentos de lenta maturação, financiar a fundo perdido os gastos na formação e manutenção de recursos humanos, regular e arbitrar os conflitos sociais e econômicos.

Paralelamente, outra contribuição significativa para o desenvolvimento, constituição e consolidação da Gestão da Informação veio, em 1934, com as contribuições de Paul Otlet **&** Henri La Fontaine que sistematizaram a documentação através do *Traitè de Documentation*.

> "[...] para Otlet, o documento é o centro de um processo de comunicação complexo, da acumulação e transmissão do conhecimento, da criação e evolução das instituições" (RAYWARD, 1991, p. 137 *apud* BARBOSA, 2008, p. 1-25).

Destarte, a perspectiva do documento enquanto informação é também destacada por Rendón (2008) que postula como objeto da Ciência da Informação o sistema informativo documental formado pela interação entre informação, documento, usuário e instituição informativa documental.

A segunda guerra mundial trouxe consigo uma demanda significativa de informações, cuja decorrência foi o fenômeno *explosão informacional*. Em 1945, Vannevar Bush, cientista encarregado de buscar soluções para o problema de informação relacionado ao excesso de informação e falta de organização, identificou e

definiu o problema de tornar acessível um acervo constante de conhecimento e propôs a criação de uma máquina capaz de associar ideias, denominada *Memex*.

No pós-guerra, a gestão da informação focava a ordenação, organização e o controle de uma enormidade de informações que era a necessidade da sociedade naquele momento e cujas ferramentas e teorias da época não tinham uma solução desenvolvida.

Uma importante contribuição nessa época, trazida pela Gestão da Informação, foi a inserção de indicações bibliográficas em detrimento dos indicadores de conteúdo do documento como um todo.

> Assessorava esse ocultamento da informação um universo simbólico privado, uma metalinguagem usurpada da linguagem natural; uma linguagem controlada, no pressuposto de que, usando-se menos palavras para identificar o documento na entrada, sua recuperação seria facilitada na saída. A era da gestão trouxe o esplendor das classificações, indexações, tesauros, medidas de eficiência na recuperação do documento como *recall and precision* (BARRETO, 2006, p.11-12)

Frederic Hayeck (1945) detecta outro problema presente na sociedade daquela época – o conhecimento disperso, ou seja, incompleto, haja vista que cada indivíduo detém uma parte separadamente. Este acontecimento, segundo Barbosa (2008) não era possuído por ninguém em sua totalidade, haja vista que ele se encontrava disperso em cada membro da sociedade e que cuja importância só era conhecida por cada um desses indivíduos.

Acredita-se que esse seja um dos interesses para que alguns anos mais tarde, na década de 60, fossem encontrados os principais autores e atores do cognitivismo ou da ciência da cognição, estudando o comportamento assimilado por conhecimento em seres humanos, máquinas e a interação entre os dois. Assim, com o cognitivismo fazendo parte das perspectivas da Ciência da Informação, a condição humana passou a priorizar a geração de conhecimento no indivíduo a partir da informação.

> Na Ciência da Informação, o cognitivismo chegou na década de 1970, introduzido por Belkin, Wersig & Nevelling […] e por projetos diversos […]. A geração de conhecimento é uma reconstrução das estruturas mentais do indivíduo realizada através de suas competências cognitivas, ou seja, é uma modificação em seu estoque mental de saber acumulado, resultante de uma interação com uma forma de informação. Essa reconstrução pode alterar o estado de conhecimento do indivíduo, ou porque aumenta seu estoque de saber acumulado, ou porque sedimenta saber já estocado ou porque reformula saber anteriormente estocado (BARRETO, 2006, p.12-13).

As mudanças começaram a ocorrer velozmente e alguns anos mais tarde, nas décadas de 70 e 90, Gómez (2000) relata que os produtos e serviços de informação ganharam notoriedade, assim como os mercados baseados na informação expandiram e se solidificaram. Inovações tecnológicas eram amplamente demandadas pela sociedade, principalmente no que concerne ao tratamento automatizado de linguagem natural, sistemas especialistas e conexão dos sistemas de informação e dos modelos de usuários.

Observa-se através dessa cronologia uma mudança de paradigma na abordagem da Gestão da Informação, haja vista que as tecnologias da informação não eram mais os elementos determinantes na sociedade e sim o conhecimento, ou seja, o que efetivamente foi assimilado das tecnologias e gerou desenvolvimento e crescimento à sociedade.

Assim, quando ocorre a mudança da perspectiva de visão da informação que antes era relativa à gestão de estoques de informação, conforme visto, passando para uma análise da ação da informação nos indivíduos, na sociedade, há necessidade de estabelecer novos parâmetros de gestão e, desta vez, com o indivíduo no centro do processo.

Esta mudança de foco propicia que a expressão gestão do conhecimento atraia mais atenção, principalmente a partir do início da década de 1990. Nesta década, segundo as autoras Nehmy **&** Paim (2003), houve dois aspectos marcantes na estrutura econômica contemporânea: a mudança no regime de acumulação no sentido de flexibilização da produção, do mercado e da força de trabalho e a globalização – já aparecem suficientemente amadurecidos, configurando os modos de inserção e de competição das empresas no mercado.

Outra característica importante é que o conhecimento obteve nova perspectiva a partir do desenvolvimento e da consolidação da internet e da web, haja vista que a rede viabiliza o acesso a conteúdos informatizados renovando as possibilidades de circulação e o acesso remoto a determinadas informações.

Kira Tarapanoff (2006) salienta que com a intensificação do uso da informação para fins estratégicos, percebeu-se que o valor da empresa, na percepção do usuário e do mercado, incorpora aspectos intangíveis tais como valor da marca, peso das patentes geradas, capacidade de inovação, talento dos funcionários etc. Através dessa percepção, a gestão do conhecimento pavimentou seu campo de atuação, pois mescla informação e conhecimento em prol do desenvolvimento e da competitividade.

Nesse novo contexto, o conhecimento ganha posição de destaque sendo um novo recurso econômico. Através da globalização e das tecnologias da informação as empresas extrapolam os limites físicos e tornam-se acessíveis para toda sociedade, sem fronteiras geográficas. Wilson (2006) define conhecimento:

> Conhecimento é definido como aquilo que sabemos. Conhecimento envolve os processos mentais de compreensão, entendimento e aprendizado que passam na mente e apenas na mente, independe de interação com o mundo exterior à mente e a interação com os outros […] o conhecimento construído a partir de mensagens nunca poderá ser exatamente o mesmo que aquele vindo da base do conhecimento que emitiu a mensagem (WILSON, 2006, p.38)

Alvarenga Neto (2008) completa que a gestão da informação é um dos componentes da gestão do conhecimento, haja vista que inclui aspectos de criação, uso e compartilhamento de informações e conhecimentos e criação do contexto capacitante ou contextos adequados para que o aspecto de criação, uso e compartilhamento se desenvolva, dentre outras frentes.

Barreto (2006) pontua que a relação entre informação e conhecimento só se realiza se a informação, instrumento modificador da consciência do homem e de seu grupo, for percebida e aceita pelo receptor, de forma a acrescentar um novo saber; sedimentar ou modificar o saber já estocado, colocando o indivíduo num estágio melhor de desenvolvimento.

Nonaka **&** Takeuchi (1997, p. 68-69) apontam quatro modos de conversão do conhecimento. Esses modos combinam duas formas do elemento conhecimento que são "o conhecimento tácito e o conhecimento explícito que interagem nos seres humanos. Os modos de conversão são através da socialização, externalização, internalização e combinação".

De acordo com os autores, a ideia de conversão do conhecimento pode estar de acordo com o modelo ACT (*Adaptative Control of Thought)* desenvolvido pela psicologia, que defende que para as habilidades cognitivas se desenvolverem, todo conhecimento declarativo, que corresponde ao conhecimento explícito em nossa teoria, tem que ser transformado em conhecimento processual, que corresponde ao conhecimento tácito.

> O modelo ACT - *Adaptative Control of Thought* - é constituído por uma memória de trabalho (onde estão representados a situação corrente da memória e os resultados dos tratamentos de informação), uma memória declarativa permanente e/ou uma memória

> procedimental permanente. A primeira armazena e organiza informações concretas e conceptuais numa rede semântica. A segunda armazena processamentos que tomam a forma de regras de aplicação que, por sua vez, permitem elaborar novos conhecimentos declarativos ou transformar antigas regras, já armazenadas (CAEIRO, 1990).

Dentro do aspecto de necessidades de informação do usuário, enfatizando especificamente o aspecto do compartilhamento do conhecimento - sendo que nesse caso o compartilhamento é visto como uma forma de proceder a busca de informação em um indivíduo, ou seja, aquisição de conhecimento tácito. A definição apontada por Alvarenga Neto (2008) é que na conceituação de compartilhamento do conhecimento, o conhecimento não é caracterizado propriamente como objeto, mas como processo. Esta linha de caracterização de conhecimento está em conformidade com a proposta de Nonaka **&** Takeuchi (1997), uma vez que ambas enxergam o conhecimento no âmbito do processo.

Ao vincular os termos gestão, informação, conhecimento e compartilhamento sob a ótica das organizações, Sianes (2006) coloca:

> Administrar o comportamento informacional, portanto, é condição básica para qualquer organização conhecer o que se sabe e poder utilizar esse conhecimento no processo de tomada de decisão e na definição de suas ações estratégicas (SIANES, 2006. p.262)

Uma vez que informação e conhecimento, segundo Davenport (1998), são essencialmente criações humanas, e nunca seremos capazes de administrá-los se não levarmos em consideração que as pessoas desempenham, nesse cenário, um papel fundamental, observa-se que ocorre a integração de realidades sociais no ambiente organizacional.

Choo (2006) destaca que, no processo de busca e uso da informação, o valor da mesma reside no relacionamento que o usuário constrói entre si mesmo e determinada informação. Assim, vários elementos afetam os padrões de busca informacional e o comportamento informacional como um todo como, por exemplo, a variedade de fontes de informação, os tipos diferentes de usuários, as necessidades e preferências dos usuários etc.

A importância do aspecto humano destacado por Choo (2006) coloca a informação como uma construção subjetiva criada dentro da mente dos usuários, ou seja, o valor da informação é construído a partir do relacionamento deste usuário com a

informação. A necessidade de busca e uso da informação é um processo de construção de significado (Choo, 2006).

Diante da multiplicidade de fatores, tanto de natureza individual quanto organizacional, que determinam o uso da informação em ambientes empresariais, Davenport (2001, p.41) afirma que administradores, no ambiente organizacional, tendem a obter de fontes humanas dois terços da informação que usam. No outro terço encontra-se a informação estruturada. Esta afirmação ratifica que, nas fontes de informação presentes na atualidade, as fontes pessoais continuam a ser as mais acessadas e confiáveis na empresa, fato este que promove o elemento humano no contexto organizacional como elemento dotado de importância e relevância.

Para dar sequência ao estudo, propõe-se que a partir de agora a segurança da informação seja relida na ótica dos elementos centrais – pessoas, processos e tecnologia. As conexões estabelecidas anteriormente ajudaram na compreensão das perspectivas centrais de cada tema. Assim, na seção 3.1 será abordado o fator pessoas – controles informais da segurança da informação. Na seção 3.2 trar-se-á uma contribuição no que concerne aos processos, ou seja, controles formais, e, por fim, na seção 3.3 será abordado o aspecto técnico da segurança da informação.

3.1 – Pessoas e Segurança da Informação: Abordagens Preliminares

No cenário empresarial, a concepção acerca do que vem a ser segurança vem evoluindo e não mais se restringe apenas à questão técnica. As demandas empresariais vêm de encontro à necessidade de se encontrar soluções estratégicas para seus negócios. Nessa perspectiva, a Segurança da Informação surge como recurso relevante, que busca atrelar ao negócio da empresa as variáveis segurança e proteção dos ativos informacionais como elementos integradores do negócio principal, uma vez que salvaguardar as informações é fundamental para o sucesso, competitividade e sobrevivência no mercado globalizado.

A tentativa desse estudo é chamar a atenção para a necessidade de se contemplar pessoas, processos e tecnologias como variáveis que coexistem nas empresas e que precisam ser tratadas, na gestão de segurança da informação, com equilíbrio e igualdade

de condições. Sveen, Torres & Sariegi (2009), por exemplo, defendem uma abordagem holística da segurança da informação e ratificam essa concepção, afirmando que os controles técnicos devem ser equilibrados com o desenvolvimento adequado dos processos, investimentos em educação formal e controles informais, com atenção especial à produção de conhecimento.

Mudar para este viés de análise implica em deixar a dependência exclusiva dos aspectos tecnológicos e dar atenção devida à subjetividade inerente aos seres humanos, suas relações e seu comportamento informacional nas organizações que tanto influenciam na gestão de segurança informacional. Colwill (2010) pontua que o excesso de confiança na tecnologia, sem a consideração de outros fatores, pode ter resultados desastrosos para gerenciar a ameaça interna, ou seja, o elemento humano presente dentro das empresas. Esta variável humana representa riscos à segurança organizacional devido ao fato desta obter acesso legítimo aos meios e informações, conhecer a organização e saber a localização de bens valiosos.

Esse capítulo será dedicado ao elemento pessoas – carro chefe dessa pesquisa. A tentativa é levantar na literatura observações acerca de como os aspectos humanos interferem na segurança da informação, ou seja, aspectos intrínsecos à condição humana, o comportamento das pessoas, suas relações e condutas que possam afetar o ambiente empresarial no que concerne ao espectro da segurança da informação. Pretende-se, ao obter tais informações, elucidar parte do problema desta pesquisa trazendo contribuições importantes para este estudo.

3.1.1- Segurança da Informação e Gestão de Recursos Humanos: Perspectivas de Modelagens Gerenciais

As empresas se organizam em mercados globais para manter a competitividade e seu padrão de vida. Uma ferramenta importante nesse processo são os sistemas de informação que agem nas organizações promovendo ações mais eficientes, em menor tempo e mais assertivas. A perspectiva de um sistema de informação não se restringe aos aspectos técnicos, mas engloba um conjunto de componentes inter-relacionados que trabalham juntos para coletar, recuperar, processar, armazenar e distribuir informações,

com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório nas organizações.

A tecnologia é o catalisador que abastece de eficiência e eficácia as empresas. Entretanto, por mais sofisticada que seja uma solução tecnológica, esta será apenas um elemento do processo de manter a competitividade e o padrão de vida da organização. Pessoas e processos são elementos críticos para todas as ferramentas, e, somente uma gestão estratégica englobando todos os componentes da organização como planejamento, ação efetiva e tratamento estratégico da informação podem trazer a competitividade que a empresa necessita.

Dessa forma, ao pensar sobre como os recursos humanos interferem na segurança da informação de uma organização, nota-se que o elemento "pessoas" é vulnerável. Esta vulnerabilidade pode ser descrita através de duas interdimensões, sendo que ambas interferem negativamente na segurança da informação e tornam o fator humano o elo mais fraco. Em primeiro lugar, os colaboradores devem, idealmente, ter conhecimento suficiente sobre a segurança da informação para a efetiva implementação e manutenção dos controles de segurança, que por sua vez contém várias informações. Em segundo lugar, os colaboradores devem ter a atitude correta em relação à segurança da informação (NIEKERK **&** SOLMS, 2010).

Esta primeira abordagem traz a reflexão a respeito da necessidade de transparência, gestão e comunicação eficaz no que diz respeito às diretrizes de segurança da informação que uma empresa adota. Todos os elementos da organização devem estar envolvidos de forma sinérgica, para que saibam lidar com as questões de segurança, desenvolvendo completude de ações e verdadeira conscientização no que concerne à necessidade de se salvaguardar os ativos organizacionais.

Kraemer, Carayon **&** Clem (2009) contribuem com essa perspectiva observando que os usuários não são, necessariamente, contrários à segurança, mas muitas vezes são incapazes de determinar as implicações de suas ações na segurança.

Este panorama remete à reflexão sobre como a falta de conhecimento gera condutas inapropriadas diante das ações de segurança da informação esperadas, uma vez que o *agir* se desenvolve exclusivamente a partir da prerrogativa do *saber como agir*. Por isso, é importante que as organizações dediquem especial atenção à manutenção e compartilhamento de informações sólidas e confiáveis, na gestão da informação e do conhecimento corporativo e no entendimento das necessidades de seus usuários.

Os usuários da informação devem ser percebidos como aqueles que não são apenas impulsionados a buscar informações para fins cognitivos e sim como entes que vivem e trabalham em ambientes sociais (como as empresas), e que através destes criam suas próprias motivações para buscar informações e satisfazer suas necessidades (WILSON, 2006 b). Este usuário da informação é definido, para esse estudo, como aquele que é fortemente dependente da informação e a utiliza com fins específicos, como por exemplo, com finalidade profissional (MEADOW,1992).

Esse processo de busca de informações, segundo Marchionini (1998), é direcionado pelo processo de necessidade informacional do indivíduo. A extrema variedade de necessidades informacionais dos indivíduos torna complexa a tarefa de enumerá-las (ALLEN, 1996).

Choo (2006) complementa a reflexão de Marchionini (1998) e Allen (1996), destacando que no processo de busca e uso da informação o valor da mesma reside no relacionamento que o usuário constrói entre si mesmo e determinada informação. Assim, vários elementos afetam os padrões de busca informacional e o comportamento informacional como um todo, como por exemplo, a variedade de fontes de informação, os tipos diferentes de usuários, as necessidades e preferências dos usuários etc.

A importância do aspecto humano destacado por Choo (2006) coloca a informação como uma construção subjetiva criada dentro da mente dos usuários, ou seja, o valor da informação é construído a partir do relacionamento deste usuário com a informação. Dentro dessa perspectiva, a escolha de fontes de informação por determinado usuário é orientada de acordo com suas preferências, necessidades, acessibilidade, ambiente, etc. Choo (2006) ainda destaca, ampliando a análise, que a escolha de uma fonte de informação é determinada através do binômio custo (acessibilidade física e o custo psicológico) versus resultado (qualidade técnica e confiabilidade); e ainda, que as fontes de informação são classificas nas seguintes categorias: internas e pessoais, internas e impessoais, externas e pessoais, e, externas e impessoais.

Para entender essas classificações Pereira (2008) propõe a seguinte síntese:

> Fontes externas pessoais: clientes, fornecedores, amigos, contatos telefônicos e outras modalidades de relacionamentos pessoais;
> Fontes externas e impessoais: publicações em periódicos e em outros meios de comunicação, conferências, convenções, relatórios de consultoria;
> Fontes internas pessoais: superiores, subordinados hierárquicos, colegas de trabalho;

> Fontes internas impessoais: relatórios internos, reuniões programadas, memorandos internos e similares (PEREIRA, 2008, p.40).

Pereira (2006) complementa a análise sintetizando que as fontes estruturadas são sinônimas de fontes impessoais, fontes estas que são, na maioria das vezes, de caráter documental ou formal. As fontes não estruturadas, que são sinônimas de fontes pessoais, são fontes que se caracterizam por proporcionar a troca de informações entre pessoas.

No contexto organizacional, as fontes de informação são utilizadas com o objetivo de levantar variáveis a respeito de aspectos ou elementos específicos do ambiente empresarial. Nesse contexto Barbosa (2006) ao fazer leitura de SUTTON (1988), identifica as seguintes fontes como as mais importantes para os gerentes americanos:

> Fontes internas: setores de vendas, de pesquisa mercadológica, de planejamento, de engenharia, de compras, análise de produtos dos concorrentes, ex-empregados concorrentes;
> Contatos diretos com o setor de negócios: clientes, encontros, demonstrações de vendas, distribuidores, fornecedores, associações comerciais, consultores, varejistas, empregados dos concorrentes, agências de publicidade;
> Informações Publicadas: periódicos do setor, material promocional das empresas, relatórios anuais, relatórios de analistas financeiros, periódicos financeiros, discursos de gerentes, periódicos de negócios, jornais nacionais e locais, diretórios, publicações governamentais;
> Outras fontes: analistas financeiros, bases de dados eletrônicas, bancos de dados de investimentos e comerciais, e anúncios (BARBOSA, 2006, p. 93)

Para finalizar, Choo (2006) ressalta que as necessidades e os usos da informação devem ser analisados dentro da situação profissional, organizacional e social nas quais os usuários estão inseridos, haja vista que elas variam de acordo com a profissão ou o grupo social do usuário, suas origens demográficas e os requisitos específicos da tarefa que este usuário está executando:

> [...] Uso da informação engloba ou deve englobar a totalidade da experiência humana: os pensamentos, sentimentos, ações e o ambiente onde se manifestam... O usuário da informação é uma pessoa cognitiva e perceptiva; de que a busca e o uso da informação constituem um processo dinâmico que se estende no tempo e no espaço; e de que o contexto em que a informação é usada determina de que maneiras e em que medida ela é útil (CHOO, 2006, p.83).

Observa-se que nesse processo de necessidade e busca informacional, o recurso disponibilizado através das informações eletrônicas, estruturados em vários caminhos, estão se tornando um ambiente dominante e o engajamento entre a relação daquele ente que busca a informação, a rede mundial, as bibliotecas digitais e outras estruturas de informação se torna a cada dia mais forte (WILSON, 2006 c).

Com a presença cada vez mais marcante dos recursos tecnológicos no nosso dia-a-dia, e, principalmente da internet, torna-se relevante trazer a este estudo a análise de Pereira (2006) que inclui, além das quatro categorias de fontes de informação mencionadas por Choo (2006), mais outras duas que são as fontes eletrônicas e não eletrônicas.

Assim, segundo Pereira (2006, p.79-80), as fontes eletrônicas são as informações obtidas através da internet, CD-ROM´s, bases de dados on-line etc., e, as fontes não eletrônicas são as informações em papel. Diante do desdobramento proposto por Pereira (2006) e Brum **&** Barbosa (2009), especificamente sobre a Internet enquanto fonte eletrônica, acredita-se que:

> A Internet, como fonte de informação, pode ser dividida em vários setores, ou seja, há muitas formas de se ter acesso à informação pela grande rede, sendo elas: listas de discussão, correio eletrônico (e-mail), informativos via correio eletrônico (newsletter), informativos comerciais via correio eletrônico (e-mail marketing), salas de bate-papo virtual (chat), mensageiros instantâneos (*instant messengers*), sítios de busca ou ferramentas de busca, intranets, extranets e os próprios sítios (sites) disponíveis na web (BRUM **&** BARBOSA, 2009. Acesso em: 25/06/2010)

Mesmo considerando a amplitude de possibilidades de busca de conteúdo pela internet, Pereira (2006) conclui que, apesar das fontes eletrônicas serem as mais utilizadas, as fontes pessoais ainda são consideradas as mais relevantes e confiáveis.

Nota-se que visão de Pereira (2006) é ratificada por Barbosa (2002) que promove estudo com o intuito de identificar as fontes informacionais para empresas, nesse âmbito realiza estudo no qual participaram 91 profissionais brasileiros. A conclusão é de que, apesar dos vários aspectos evidenciados com o uso crescente da tecnologia, as pessoas continuam a ser as fontes mais utilizadas e aquelas vistas como mais relevantes.

Por isso, o entendimento sobre necessidades informacionais de usuários perpassa pelo comportamento de busca da informação que resulta do reconhecimento de alguma necessidade percebida pelo usuário. Este comportamento pode ser determinado de

várias formas, seja através de demandas do usuário sobre os sistemas formais que são comumente nomeados de sistemas de informação, pleitos sobre sistemas que podem desempenhar funções de informação agregada a uma função primária ou não primária e, por último, a busca de informação através de outra pessoa, cuja conotação pode ser descrita como troca informacional (WILSON, 2006 b).

Assim, a partir das necessidades informacionais dos usuários da informação que atuam no meio corporativo, busca-se compreender como essas pessoas preservam a informação. Esse é o interesse de reflexão da presente pesquisa. Entretanto, vale ressaltar o posicionamento de Wilson (2006 b), quando afirma que investigar os usuários da informação no mundo corporativo não é proveitoso, haja vista que o mundo empresarial oferece contextos de uso da informação que diferem entre si.

Apesar desse posicionamento, continua-se com a investigação e, pode-se observar que são as necessidades de informação um dos pontos de partida para que usuários demandem e empreguem sistemas de informação e serviços, e, forneçam os critérios através dos quais o desempenho tanto dos sistemas de informação quanto dos serviços possam ser avaliados. Paralelamente, a busca informacional é o comportamento passível que evidencia as necessidades de informação e a única base na qual se pode estabelecer julgamentos acerca da natureza da necessidade informacional e sua respectiva satisfação. Unindo essas perspectivas, pode-se concluir que as necessidades informacionais são construtos explanatórios que ajudam a entender o comportamento informacional (ALLEN, 1996).

Esse pensamento nos faz perceber que, ao construir um comportamento de segurança da informação em uma organização, trabalhar-se-á com elementos de estudo pertinentes à ciência da informação e que esses elementos alimentam uma trajetória que se inicia com a necessidade de informação, passa pela busca informacional e termina com o comportamento informacional.

Por isso o comportamento de necessidade, busca e uso informacional é um processo de construção de sentido. O usuário constrói o significado a partir das informações encontradas, passando da incerteza e da indefinição para a clareza e a confiança (CHOO, 2006). A construção de sentido, segundo Alvarenga Neto (2008) possui as seguintes características de propriedade e natureza:

> Construção de sentido fundamentada na construção de identidade: ela é necessária para que o indivíduo mantenha uma autoconcepção

> consistente, e é frequentemente iniciada quando o indivíduo falha em confirmar essa autoidentidade;
> Construção de sentido retrospectiva: aqui, o problema principal é escolher um significado que seja plausível a partir de vários significados possíveis, com o propósito de interpretar eventos passados;
> Construção de sentido representada: as pessoas em organizações frequentemente produzem parte do ambiente que enfrentam;
> Construção de sentido social: ela é feita em grupos;
> Construção de sentido fluida: ela não começa e nem termina mas é continuamente presente no fluxo de atividade, projetos e processos que constituem a vida organizacional;
> Construção de sentido focada em e extraída de pistas ou dicas: são os pontos de referência a partir dos quais os elos e os nós são ligados e conectados às redes de significado;
> Construção de sentido dirigida pelo razoável ou aceitável que pela precisão: com a nova dinâmica e a velocidade das operações empresariais, as pessoas tendem a trocar a precisão pela velocidade (ALVARENGA NETO, 2008, P.82,83).

Doravante, ao pensar sobre a questão das pessoas terem um comportamento seguro, sugere-se que uma das formas para conseguir tal propósito seria proporcionando esclarecimentos adequados acerca do que vem a ser um comportamento seguro, o que é segurança da informação, formas através das quais se consegue minimizar os riscos, como salvaguardar os ativos informacionais corporativos e como se posicionar para se preservar de ataques.

Andalécio **&** Souza (2008) contribuem com essa reflexão quando, em uma leitura da obra de Jean Piaget, colocam que o conhecimento tem como meta ou propósito específico ajudar a pessoa a adaptar-se ao ambiente (p.76). Nesse sentido, existem três mecanismos que produzem este processo de adaptação, segundo Piaget:

> Assimilação (esforços do indivíduo para lidar com o ambiente, fazendo-o ajustar-se às estruturas existentes em seu próprio organismo – por incorporação);
>
> Acomodação (tendência do indivíduo de mudar em resposta às exigências do ambiente);
>
> Equilibração (esforços do organismo para atingir equilíbrio em suas interações com o ambiente, utilizando os mecanismos anteriores).
>
> Estes mecanismos atuam ao longo de toda a vida do indivíduo (ANDALÉCIO **&** SOUZA, 2008, p.76).

Diante da junção das perspectivas expostas pelos autores, entende-se que há necessidade de desenvolver conhecimento e assegurar informações junto às pessoas, haja vista que nota-se que, no ambiente corporativo, empregados, intencionalmente ou

por negligência, muitas vezes devido à falta de conhecimento, são a maior ameaça à segurança da informação.

A conscientização das pessoas sobre a importância de um nível adequado de cooperação do usuário e do compromisso com a construção de conhecimento é preponderante, haja vista que, sem tais contribuições, as técnicas de segurança são passíveis de serem mal utilizadas ou mal interpretadas pelos usuários, se tornando ineficazes. Por esse motivo é que a segurança das informações depende tanto do conhecimento humano quanto da cooperação humana. A expectativa é que a falta de conhecimento possa, na maior parte dos casos, ser tratada através da educação, enquanto a falta de cooperação possa ser abordada através da promoção de uma subcultura de segurança da informação na organização (NIEKERK **&** SOLMS, 2010).

É compreensível que essas abordagens nos levem a pensar em como os fatores conhecimento e cooperação por parte das pessoas são complementos críticos à variável humana na gestão de segurança informacional. Analogamente, elementos como compartilhamento de conhecimento, aprendizagem organizacional e gestão do capital intelectual trazem tônus à abordagem proposta e propiciam amplitude de visão e desenvolvimento de ações organizacionais abrangentes para gerir os recursos humanos.

Não obstante, percebe-se o quanto as pessoas precisam ser encaradas como possíveis variáveis promotoras de risco no ambiente corporativo, pois através dessa percepção, mais rapidamente, as brechas de segurança geradas por essas pessoas podem ser entendidas e as devidas ações implementadas.

Uma brecha de segurança envolve a necessidade de antecipar o futuro e contextualizar as ocorrências, visando mais precisão e menos abordagens reativas frente a problemas de segurança, ou seja, mais ações visando a prevenção e menos visando a correção.

Marchionini (1998) ressalta que as ações reativas requerem a percepção de inputs de informações e relativamente o resgate de informações da memória, ou seja, percebe-se a situação através dos sentidos e automaticamente determinam-se reações de acordo com os modelos mentais existentes. Já as ações previamente pensadas (proativas) são conduzidas por planos, empregam saídas de informação, o recolhimento da informação ativa e requerem síntese da informação.

Complementar a essa visão, Andalécio **&** Souza (2008) colocam que a aquisição de conhecimento influencia os sistemas de educação e que a cognição modifica o

comportamento do indivíduo através de aquisição de novas associações, informações, insights, aptidões, hábitos etc. Assim, o processo de mudança de comportamento, segundo Andalécio **&** Souza (2008), ocorre segundo os seguintes aspectos:

> Condicionamento respondente, condicionamento operante e observação. Um condicionamento é a criação de uma nova associação entre um sentimento, estado fisiológico ou ação, de um lado, e um evento que constitui um estímulo, do outro.
>
> O condicionamento respondente, ou clássico, envolve um comportamento reflexo, o qual pode ser condicionado pela associação do estímulo que o elicia a um outro que não exerce esse papel e que, ao final de um período de tempo, também passará a provocar essa resposta automática (controle pelos antecedentes).
>
> No condicionamento operante, a frequência de ocorrência de um comportamento operante (um ato iniciado voluntariamente pelo indivíduo) é modificada (aumentada ou diminuída) pelos eventos que seguem esse comportamento (controle pelas consequências). Se estes eventos forem agradáveis para o sujeito (reforço), é provável que o comportamento se repita mais frequentemente. Já se as consequências forem desagradáveis (punição), o comportamento tem probabilidade de ser repetido com menor frequência.
>
> Dentro desta abordagem, a mudança de comportamento pode ser causada também pela observação dos atos de outro indivíduo, processo que recebe várias denominações: aprendizagem por observação, aprendizagem vicariante, aprendizagem social, modelação ou imitação (ANDALÉCIO **&** SOUZA, 2008, p. 75 e 76)

Outro ponto importante mencionado por Andalécio **&** Souza (2008) é que através do processamento da informação, o indivíduo, no caso desse estudo o usuário da informação, avaliará se o recurso empregado por ele na solução de um ou mais problemas foi suficiente e obteve sucesso ou não. Nesse caso, se não obteve sucesso ocorre o processo de reorganização do conhecimento e mudança de comportamento.

Destarte, as considerações dos autores promovem campo fértil para se refletir sobre a conexão que existe entre a necessidade de o colaborador ter consciência acerca da gestão de segurança da informação e seu papel nesse processo, sobre quais passos seguir para se ter uma conduta segura, sobre o imperativo de se conhecer as políticas de segurança da informação da empresa e aplicá-la na sua conduta do dia-a-dia, sobre a condução de práticas de gestão do conhecimento como, por exemplo, a socialização para difundir boas práticas e assim promover um espaço para relatar ataques e como lidar com eles, expor possíveis riscos, ameaças, ações adotadas pela empresa para garantir o segurança de seus ativos, promover a aprendizagem organizacional etc., de modo que os esforços da empresa estejam focados em permitir a aquisição de

conhecimento por parte do colaborador e, consequentemente, a mudança de comportamento.

Fazendo uma conexão com uma abordagem já realizada no texto, percebe-se que nas ações preventivas há um comportamento de busca informacional em fontes diversas para sanar determinada necessidade e, que quando se planeja com detalhes formas para alcançar um objetivo, um conjunto de ações são propostas e ele modifica o comportamento informacional dos colaboradores. Há de se fazer notar que uma variável importante nesse contexto é o tempo, mesmo porque em vários casos não há tempo suficiente para se impetrar medidas preventivas, e, por esse motivo são adotadas medidas corretivas. Adverte-se, porém, que ainda no caso de medidas corretivas, a base para as ações são os modelos mentais existentes, essa visão ratifica mais uma vez a importância de se promover o desenvolvimento do conhecimento, da cooperação e da aprendizagem organizacional entre os colaboradores, visando a disseminação de informações sobre segurança da informação, de modo a fazer com que a informação chegue antes que seja necessária uma atitude corretiva por parte de quaisquer pessoas da empresa. Nota-se, entretanto, que Colwill (2010) aponta que são necessárias muito mais ações preventivas que corretivas.

Outros pontos relevantes e que são importantes de lembrar é que para se ter um equilíbrio, tanto frente à abordagem preventiva quanto à corretiva, deve-se contar com características individuais de cada pessoa, suas experiências além da estabilidade e organização do ambiente (Marchionini,1998).

Ressalva-se, inclusive, que os modelos de avaliações de riscos podem ajudar na tarefa de promover o desenvolvimento do conhecimento, uma vez que eles podem ser vistos como mecanismos de aprendizado, sendo auxiliadores no processo de aprendizagem organizacional. Fazendo uma correlação entre avaliação de riscos e aprendizagem organizacional, vale ressaltar que, se a percepção de segurança através da avaliação de risco aumenta, a empresa aprende mais e, consequentemente, a taxa de aprendizagem e o corpo de conhecimento em segurança da informação aumentam, reforçando a capacidade da empresa de detectar falhas de segurança e dos funcionários agirem de forma mais consciente (SVEEN, TORRES **&** SARIEGI, 2009).

Ao fazer um apanhado de todos os pontos até o momento discutidos, percebe-se que, ao compreender os recursos humanos como ameaça no âmbito da segurança da informação e, diante da impossibilidade de se erradicar tal ameaça, a alternativa

plausível e viável é se trabalhar avaliando e gerenciado os recursos humanos empresariais.

Acredita-se que a contribuição diante dessa constatação é entender as formas de avaliar e gerenciar os recursos humanos com relação à segurança da informação. Na literatura existe um debate sobre o assunto e nesse momento trar-se-á aos leitores algumas considerações sobre o tema.

Colwill (2010) explica que alguns fatores básicos característicos da ameaça humana interna ao contexto corporativo são: oportunidade, motivação e capacidade. A motivação virá dos recursos humanos internos à empresa e conduzida por eles. Já a oportunidade e a capacidade serão dadas aos novos colaboradores pela própria organização, seja através de acesso a informações para execução de suas atividades ou através de acesso encoberto e não autorizado da parte das pessoas, uma vez que estão dentro da organização. É importante que esses fatores sejam incluídos nas avaliações de ameaças internas.

Concomitantemente, há de se levar em consideração que as organizações precisam equilibrar a acessibilidade à informação para que seus colaboradores executem seu trabalho com a aplicação de níveis adequados de controle e auditoria. Desta forma, entende-se que todos os esforços para consolidar aspectos como lealdade, confiança e sensibilização das pessoas para as questões de segurança devem ser postos em prática. Todavia, um esforço adicional por parte da organização é necessário para tornar essas questões intangíveis mais compreensíveis e perceptíveis na visão dos colaboradores (COLWILL, 2010).

O descontentamento também pode ser mencionado como um dos pontos de partida para muitos funcionários acabarem atacando os sistemas de sua própria organização. Por isso uma gestão eficaz e eficiente deve focar não somente as políticas comerciais e procedimentos, cultura organizacional e ambiente técnico. O olhar da gestão organizacional deve ir além da tecnologia, de modo a atingir o negócio como um todo, inclusive os aspectos no que concerne à interação entre os processos e as tecnologias utilizadas (Beautement **&** Sasse, 2009).

Quando se fala sobre a gestão de segurança da informação participar do negócio da empresa, quer dizer que o olhar das corporações deve ser ampliado no sentido de ver que a informação é o ativo de valor que gera competitividade no mercado globalizado para essa empresa. Esse ativo informacional é processado no ambiente organizacional e

nele ganha valor agregado. As pessoas processam a informação, seja através dos sistemas de informação ou não, e por isso elas detêm parte do conhecimento daquele ativo. Almeida (2007) ressalta que uma organização não possui apenas dados em formato digital, haja vista que existem informações sobre determinada empresa armazenadas fora de seus domínios (governo, fornecedores etc.). Assim, para proteger o ativo informacional que está disperso nos sistemas, fontes, pessoas e processos organizacionais, as empresas devem se atentar para o fato de que suas estratégias de atuação devem contemplar a necessidade prioritária de proteção dos ativos informacionais corporativos e, consequentemente, seus objetivos estratégicos e seu planejamento estratégico contemplarão ações que serão executadas tanto no setor operacional, tático, quanto no setor estratégico da estrutura organizacional.

Muito se tem discutido sobre a correlação entre funcionários 'descontentes' e ataques internos. Essa questão merece um cuidado especial, uma vez que pode apenas estereotipar pessoas induzindo foco em elementos errados como, por exemplo, dirigentes sindicais e funcionários com queixas verdadeiras. Segundo Colwill (2010) a NIAC – National Infrastructure Advisor Council (2008) considera que não há correlação direta entre os trabalhadores descontentes e as ameaças internas e que a maioria dos funcionários descontentes nunca chegou perto de trair seus empregadores. Uma verdadeira análise de motivação e traição exige levantamento psicológico complexo e varia de indivíduo para indivíduo. Shaw et al. (1999) apud Colwill (2010), identificam seis características pessoais que acreditam ter implicações diretas para riscos de um potencial invasor malicioso:

- Falsa sensação de falta de reconhecimento e direito, resultando em um desejo de vingança;

- Raiva e frustrações sociais, alienação, não gostam de autoridade e possuem uma inclinação de vingança;

- Dependência do computador e solidão agressiva, desejo de explorar redes, quebrar códigos de segurança e desafiar os profissionais de segurança;

- Ética e flexibilidade sem inibições morais que normalmente impedem o comportamento malicioso;

- Redução de lealdade - se identifica mais com a sua profissão ou especialidade de computador do que com o seu empregador;

- Falta de empatia e descaso ou incapacidade de apreciar o impacto do comportamento dos outros.

Para finalizar, Colwill (2010) ainda relendo a NIAC (2008) conclui que as pessoas que cometem ações mal-intencionadas a partir de privilégios têm uma experiência de causalidade ou mecanismo que afeta a motivação e conduz à traição. Essas experiências podem ser classificadas em três fontes principais:

- O descontentamento crescente;
- Contratação por entidades exteriores hostis ou grupos;
- Infiltração de um ator de ameaça maliciosa em uma posição de confiança.

Quando se cruza esses elementos com o imperativo de desenvolver cooperação e conhecimento nas empresas, levando em consideração variáveis intrínsecas à personalidade humana, como - oportunidade, motivação, capacidade e descontentamento, previamente anunciadas, vê-se que, mais do que nunca, as organizações precisam ser estratégicas ao lidar e tratar seus recursos humanos.

As pessoas podem desenvolver sentimentos a partir de experiências e agir de forma a prejudicar a organização. Por isso é muito importante que as organizações ajam proativamente no desenvolvimento e incentivo de ações cooperativas entre os colaboradores e também entre a organização e seus colaboradores. Não obstante, há a necessidade de se promover ações que venham a contribuir com a expansão e o compartilhamento de conhecimento nas empresas, para com isso criar consciência nas pessoas e aproximá-las mais intimamente da organização.

Vale a pena destacar a perspectiva dos colaboradores confiáveis que também se respaldam na reciprocidade. Estes colaboradores dão confiança e esperam, em contra-partida, confiança e, por isso, as organizações devem estar atentas para fornecer esse equilíbrio. Agindo dessa maneira ambas serão beneficiadas, uma vez que da parte dos colaboradores haverá o compromisso com a proteção das informações sensíveis da organização e, da parte da organização, haverá direcionamentos de esforços para fornecer algum tipo de proteção (WORKMANN, 2007).

A sinergia entre organização e colaboradores é primordial na manutenção de uma cultura organizacional que tem seu cerne na segurança de seus ativos informacionais. Paralelamente, o desenvolvimento de ações cooperativas, disseminação

de conhecimento e aprendizagem organizacional são facilitadas devido à sinergia das partes.

Uma conexão adequada entre empregadores e empregados é tão importante que, de forma geral, nota-se que as organizações não podem proteger a integridade, confidencialidade e disponibilidade das informações alocadas em ambiente de sistemas em rede, sem garantir que cada pessoa envolvida compreenda seus papéis e responsabilidades e seja adequadamente treinada para realizá-los. Por isso, garantir a confidencialidade, disponibilidade e integridade das informações quer dizer:

> Integridade diz respeito à proteção contra alteração indevida ou destruição, assegurando a autenticidade e o não repúdio;
>
> Confidencialidade significa preservar restrições de divulgação e de acesso, garantindo meios para proteção da privacidade pessoal;
>
> Disponibilidade significa assegurar o acesso e o uso da informação de forma confiável (ALMEIDA, 2007, p.2).

Assim, um usuário deve estar ciente e compreender os controles operacionais específicos, uma vez que a eficiência do processo depende de seu comportamento. Para garantir esse nível de conhecimento exigido, será necessária uma formação extensiva, conscientização e programas educativos (NIEKERK **&** SOLMS, 2010).

Uma vez percebido que a segurança da informação não é apenas um problema de tecnologia e pesquisa, observa-se que, por parte das organizações, há uma concordância sobre a necessidade de mudança de comportamento dos funcionários visando alcançar níveis mais elevados de proteção, em conformidade com suas políticas de segurança da informação. Entretanto, o caminho adotado para realizar esse objetivo é equivocado, uma vez que na maior parte das vezes as empresas adotam somente uma postura de ameaça frente aos trabalhadores, impondo sanções caso as políticas não sejam seguidas (BEAUTEMENT **&** SASSE, 2009).

A perspectiva abordada pelos autores até o momento nos leva a crer que a melhor maneira de "trabalhar" os recursos humanos de acordo com as necessidades de segurança informacional da organização é trazendo esse recurso para o lado da empresa. Assim, todos os esforços para conscientizar o colaborador, desenvolver a cultura de compartilhamento de conhecimento, colaboração e aprendizagem organizacional não funcionarão se a empresa adotar uma postura de ameaça frente aos trabalhadores e se guiar pela promoção da coação e do medo dos colaboradores para com a empresa. Vale

ressaltar que uma postura de medo, coação e ameaça é bem diferente da adoção de métodos de gestão, como no caso das sanções e recompensas.

Por isso, para mudar a mentalidade dos colaboradores deve haver, previamente, uma mudança de gestão. Esta gestão deve seguir as diretrizes das propostas de uma abordagem de segurança informacional holística, tratando pessoas, processos e tecnologias concomitantemente. No caso do elemento *pessoas*, a expectativa é que a empresa esteja preparada para implementar ações que venham a contribuir com a criação de uma cultura de segurança, de modo que todos os membros de uma determinada organização levem a segurança em conta em seu trabalho diário, e não apenas como um complemento (SVEEN, TORRES **&** SARIEGI, 2009).

Deve ser lembrado que uma mudança de crenças e valores se dá a partir de resultados de processos de aprendizagem com base no comportamento de sucesso. Por isso, comentários, recompensas e sanções são mecanismos de gestão que devem ser usados de forma correta, a fim de garantir que os funcionários entendam o que seria um comportamento considerado bem-sucedido (NIEKERK **&** SOLMS, 2010).

Os autores Huang, Rau & Salvendy (2010) fizeram uma leitura da pesquisa de Fibikova **&** Vyskoc (2001) sobre como os usuários de TI veem a segurança da informação. Os resultados revelaram que os usuários nem sempre pensam da mesma maneira que os especialistas em segurança, e alegaram que a real segurança só pode ser alcançada quando os funcionários da organização colaboram em se comportar de forma segura.

Em sintonia com a necessidade de mudança do comportamento dos colaboradores, a educação aparece como uma opção de abordagem e se caracteriza, frequentemente, como a única maneira de convencer funcionários e gerentes sobre a necessidade de fazer as coisas de forma diferente. Assim, para uma mudança paradigmática na organização, é vital ensinar os funcionários o que fazer, como fazer e porque isso deve ser feito ou aquela conduta deve ser adotada (NIEKERK **&** SOLMS, 2010).

O autor Everett (2008) contribui dizendo que a formação dos funcionários e a educação são fatores preponderantes quando se fala em obter ou aumentar a conscientização acerca do valor dos dados manipulados dentro da organização e, respectivamente, do papel de cada indivíduo na organização para salvaguardar este ativo. Por isso, a conscientização deve ser um componente intrínseco da cultura

organizacional e deve ser medida antes e depois de qualquer mudança promovida na empresa. As ferramentas utilizadas para tal medição são enquetes cujos resultados provarão a compreensão acerca da mudança proposta e, mais diretamente, através dos pedidos de renovação de senha e diminuição de incidentes de acesso indevido ou não autorizado à empresa.

É substancial que os empregados percebam que a forma atual de fazer as coisas já não é boa o suficiente. Sem o descongelamento dos valores correntes, os funcionários irão resistir à mudança. Apesar da tentativa inerente ao ser humano de se manter estável, se a mudança ocorrer, este equilíbrio será perturbado e o reconhecimento desta força de mudança gerará motivação para que a referida transformação se efetive. Assim:

- Descongelamento / desconfirmação: Auditorias regulares à senha devem ser executadas e as medidas disciplinares devem ser tomadas contra os trabalhadores cujas senhas não estão em conformidade com as políticas da empresa;
- Aprendizado: Os empregados devem adquirir conhecimento acerca do que se constitui uma senha segura;
- Internalização / recongelamento: A força média de senhas de funcionários de cada departamento deve ser incluída como um indicador chave de desempenho para o gerente que departamento (NIEKERK **&** SOLMS, 2008).

O processo educativo, em geral, pode ser visto como sistemas de ensino e aprendizagem que estão ligados entre si através de vários elementos, tais como feedback, avaliação, interação, garantia de qualidade, orientação e apoio. A intenção é que todos esses componentes desempenhem um papel na criação de um efetivo programa de educação em segurança da informação (Niekerk **&** Solms, 2010).

A ISO 1799 traz diretrizes no que tange à educação e formação de colaboradores, colocando que esta deve incluir requisitos de segurança, responsabilidades legais e controles corporativos, bem como treinamento no uso correto das instalações de processamento de informação antes que o acesso a informações ou serviços seja concedido.

Entretanto, a dificuldade de construir controles informais (recursos humanos) fortes, levou à uma espécie de compensação, que se deu através da construção de controles formais (políticas, normas, diretrizes, etc.) muito fortes. Esse fato pode ser constatado pelo grande número normas de segurança de informações como, por exemplo, as normas ISO 1799 e COBIT. No entanto, não há como garantir a plenitude dos controles formais sem se desenvolver fortes controles informais. As características particulares da cultura de cada empresa impõem adequações ao conjunto de normas de segurança no ato de sua implementação. Por este motivo, há uma diferença entre o que está escrito nas normas e que é realmente praticado nas empresas (SVEEN, TORRES **&** SARIEGI, 2009).

Paralelamente, vê-se que uma otimização no âmbito organizacional perpassa pela necessidade de soluções ágeis, construção e manutenção da confiança e relações seguras ao longo do tempo. Isso requer, além de um enfoque em fatores humanos, educação, sensibilização, uma maior atenção no "pós-tratamento" da segurança de funcionários e terceiros (COLWILL, 2010).

A educação é quesito estratégico no processo de segurança da informação e requer a utilização de uma metodologia pedagógica sólida para a criação de ensino. Uma vez que os usuários tenham conhecimento suficiente sobre seus papéis no processo de segurança, ainda não há garantia de que eles irão aderir a todas as precauções necessárias. Em alguns casos, percebe-se que os usuários entendem o seu papel corretamente, mas ainda não aderem à política de segurança devido ao fato dela entrar em conflito com suas crenças e valores. Portanto, para se atingir o êxito esperado é imperativo garantir que os usuários tenham uma atitude correta e, portanto, um comportamento desejado para ações de segurança de informações (NIEKERK **&** SOLMS, 2010).

O objetivo de fomentar comportamentos de segurança da informação faz com que pessoas sejam favoráveis à proteção dos ativos de informação, de acordo com as políticas da organização, no que tange à segurança da informação e com base no código de ética. O êxito dos comportamentos de segurança geraria maiores índices de comunicação de incidentes de segurança, a adesão a uma política de mesa limpa ou eliminação de documentos confidenciais (DA VEIGA **&** ELOFF, 2010).

Os autores Huang, Rau **&** Salvendy (2010) fizeram uma leitura do trabalho de Yenisey et al. (2005) no qual se investigou os sentimentos dos usuários de segurança no

e-commerce e diretrizes desenvolvidas para percepção de segurança no comércio eletrônico. Neste estudo, a percepção da segurança da informação foi definida como o mecanismo através do qual uma pessoa avalia as ameaças à segurança da informação que, por sua vez, determinam sua resposta comportamental.

Outros estudos sobre a questão da percepção dos usuários e seus comportamentos relacionados à Segurança da Informação apontam a existência de significativa correlação entre o bom comportamento relacionado a *senhas x formação x sensibilização da organização*. Em contrapartida, identificou-se que alta carga de trabalho pode criar um conflito de interesses entre a funcionalidade e segurança da informação e que as tarefas e alta carga de trabalho estiveram associadas aos estados de sistema enfraquecido e erro humano durante uso do sistema (KRAEMER, CARAYON **&** CLEM, 2009).

Essa perspectiva abre caminho para a necessidade de cada vez mais focar a percepção das pessoas com relação à segurança da informação. Este é um importante componente da inteligência humana e uma chave para compreender o comportamento humano. Através da percepção a pessoa avalia insumos externos que, por sua vez, determinam a resposta comportamental como, por exemplo, no caso de usuários de TI que respondem a diferentes tipos de ameaças de acordo com suas percepções de segurança da informação. Elementos tais como superestimativa do risco, podem fazer com que soluções não sejam utilizadas, como por exemplo, as pessoas que se recusam a usar o internet banking devido à preocupações, necessárias e desnecessárias, com os problemas de segurança. Já a subestimação do risco pode, indevidamente incentivar as pessoas a se engajar em práticas inseguras, como por exemplo, utilizarem um conjunto simples e fraco senhas para o seu sistema de informação, haja vista que acreditam que o risco de o sistema ser atacado é baixo (Huang, Rau **&** Salvendy, 2010).

Tratar o aspecto humano da segurança da informação é ponto proeminente nesse estudo e, portanto, não há como deixar de relatar uma tendência mundial nas organizações que é o *outsourcing* (terceirização). Os colaboradores terceirizados estão sempre presentes em algum lugar da organização e são passíveis de instrução educacional para um adequado comportamento e atitude consciente, assim como os colaboradores diretos. Logicamente, a educação eficaz continuará a ser difícil em ambientes onde os fornecedores de mão de obra terceirizada estão crescendo rapidamente e contratando milhares de novos funcionários. Há de se direcionar esforços

no ambiente corporativo para centrar forças no processo educacional dos colaboradores no âmbito total da organização. Os usuários terceirizados necessitarão de formação adequada, treinamento e, em certas regiões, devem ser consideradas adicionalmente questões de ética organizacional e como esta é promovida, assim como a forma através da qual os funcionários são treinados e recompensados (COLWILL, 2010).

O treinamento e a formação geram conhecimento e consciência por parte dos funcionários e é uma ação extremamente importante por parte das empresas que, somente diante dessa constatação de ciência, podem promover novas frentes, como o desenvolvimento de novas posturas e comportamento por parte dos colaboradores (WORKMANN, 2007).

A tarefa de formação de pessoas não é fácil. Todavia, a educação desempenha um papel muito importante no estabelecimento de uma cultura no ambiente corporativo. Pode ocorrer uma falsa percepção e/ou um processo de comunicação ineficiente quando pessoas relacionam novas informações e conhecimentos juntamente com experiências e valores anteriormente aprendidos, consciente ou inconscientemente. Por isso, para determinar o comportamento dos usuários é necessário cultivar uma subcultura de segurança da informação na organização, de tal forma que esta venha a apoiar todas as atividades e projete a segurança da informação como uma ação e um aspecto natural nas atividades diárias de cada funcionário. É primordial que as pessoas sejam educadas para quererem ser mais seguras no seu dia-a-dia, e, essa transformação de atitude é de suma importância, haja vista que uma modificação de atitude conduz, consequentemente, a uma alteração comportamental (NIEKERK **&** SOLMS, 2010).

Proteger as informações de uma organização é da responsabilidade de todos os funcionários. Educação, formação e sensibilização são talvez as maiores medidas não técnicas disponíveis e comuns a uma mesma perspectiva – o *elemento humano* x *segurança da Informação*. Temas e requisitos de segurança devem ser integrados no comportamento das pessoas como uma atividade normal, através de uma política clara e de escolaridade. Muitos problemas de vazamento de informação privilegiada provêm da ignorância ao invés da má-intenção, todavia, falhas acidentais podem gerar grandes impactos.

Observa-se que, em algumas empresas, segurança e educação são quesitos obrigatórios, auditados sob a perspectiva legal e das regulamentações. Um foco de mudança necessário é medir o comportamento real da força de trabalho como parte do

desenvolvimento organizacional. A formação básica e instruções podem ser usadas, mas deve ser dado um foco maior no que concerne à integração e à sensibilização para a segurança informacional e compreensão da cultura organizacional. Os colaboradores devem mudar seu comportamento a fim de proteger os bens e informações, e para se conseguir este objetivo deve-se não apenas aumentar a sensibilização dos funcionários, mas incorporar as necessidades de segurança informacional nos valores culturais da organização.

Para ser realmente eficaz, deve-se ir além de simplesmente seguir as políticas de segurança da informação. Deve-se trabalhar em um processo de construção de empatia, compreensão, apropriação e desenvolvimento de conhecimento acerca de situações que podem causar riscos à segurança informacional, comportamentos e reações inadequadas (COLWILL, 2010).

O comportamento de segurança de informação que se mantém ao longo do tempo evolui para uma cultura de segurança da informação que é evidente em artefatos, bem como nos valores e pressupostos das corporações. A cultura de segurança da informação difere de organização para organização. Ela é influenciada pelo tipo de cultura organizacional, bem como pelos componentes de segurança da informação que são implementados e pelo comportamento organizacional em cada camada (DAVEIGA & ELOFF, 2010).

Efetivamente, culturas diferentes fazem com que processemos as mesmas informações de formas distintas. Uma impressão prematura sobre algo ou alguém pode ocasionar um impacto no comportamento daquela pessoa. Quando ocorre o processo de uma impressão marcante em alguém, essa impressão condiciona fortemente os processos de pensamento da pessoa e, respectivamente, suas ações futuras (RAPAILLE, 2007).

Assim, a forma pela qual a informação é processada no indivíduo, no grupo e consequentemente na cultura da empresa é fator de importante avaliação para solidificação de valores e paralelamente de criação de impressões marcantes nos colaboradores.

Esse dinamismo e multiplicidade de fatores nos faz pensar que os complexos culturais podem ser pensados como expressões de um sistema dinâmico de relações que atendem a necessidade individual básica para pertença e de identidade, através da ligação de experiências pessoais e expectativas do grupo. Aplicando essa ideia ao

espectro da *psiquè*, relata-se como ela se comporta ao longo dos estágios de consciência. Dessa forma, a consciência pode manifestar-se ou ser flexibilizada na direção da identificação com o comportamento da cultura coletiva ou com expressões mais individuais. Complexos culturais impõem restrições sobre a percepção de diferenças ou as acentua, enfatizando a identificação com o grupo ou a diferenciação do grupo e permitindo que os sentimentos de pertença ou alheios ao grupo se aflorem (KIMBLES, 2000).

Para entender os elementos presentes nos complexos culturais corporativos, os autores Niekerk **&** Solms (2010) trazem contribuições concernentes às subdivisões que estes adquirem no ambiente empresarial. São elas:

— Artefatos: Os comportamentos visíveis e mensuráveis no dia-a-dia da organização.

— Valores: Os documentos escritos, como uma visão ou declarações políticas, que defendem os valores formais da organização.

— Hipóteses (compartilhamento de conhecimento tácito): As crenças e valores subjacentes dos trabalhadores. Estes são os verdadeiros *drivers* de comportamento do empregado e foram formados como resultado da articulação de experiências de aprendizagem, com base no comportamento passado de sucesso.

Entretanto, Colwill (2010) chama nossa atenção quando diz que pelo menos duas perspectivas culturais devem ser consideradas quando se examina a ameaça interna à organização: a cultura organizacional e cultura nacional/regional. Diferenças regionais e culturais que se manifestam em diferentes perfis de segurança, de ameaça e de risco e podem ter impacto sobre comportamento e a eficácia dos níveis de proteção de informação.

A cultura de segurança informacional, ou seja, percepções, atitudes e pressupostos que são aceitos e encorajados em uma organização - assim como o modo pelo qual as coisas são feitas em uma organização para proteger os ativos de informação, se desenvolve como um resultado da interação dos colaboradores com informações e controles de segurança, tais como senhas, cartões de acesso ou software antivírus. Uma cultura de segurança da informação pode ser definida como a maneira como as coisas são feitas na organização para proteger os ativos de informação (DA VEIGA **&** ELOFF, 2010).

Ainda com relação à cultura de segurança da informação, os autores Kraemer, Carayon **&** Clem (2009) ressaltam que a perspectiva da cultura de segurança foi desenvolvida para ser multidimensional, incluindo governança da segurança, controle, coordenação, processos de segurança, apoio à gestão, participação e formação dos funcionários e conscientização dos colaboradores sobre segurança.

O fato é que a interação entre os componentes de segurança de informação, tais como política e comportamento dos funcionários, tem impacto sobre dois outros componentes - comportamento de segurança da informação e de cultura de segurança da informação. O conjunto de componentes de segurança da informação pode ser agrupado em categorias que são implementadas pela organização sobre o indivíduo, grupo ou nível organizacional, influenciando comportamentos de segurança da informação (DA VEIGA **&** ELOFF, 2010).

Para alterar os valores de uma pessoa, crenças, atitudes ou estados psicológicos ou mentais, mais que apenas a educação será necessária. A "força" de convicções e valores também terá um grande impacto sobre quão fácil ou difícil será mudar essas crenças e valores (NIEKERK **&** SOLMS, 2010).

O comportamento organizacional e informacional do cidadão envolvendo os aspectos de papéis informais e relações de trabalho pode ser gerenciado através de "contratos psicológicos" negociados com os trabalhadores, ao invés de depender uma abordagem de comando e controle. Políticas de uso aceitável e orientações podem ser utilizadas para facilitar tais contratos. Mudança de cultura deve também servir para a diversidade regional e questões que afetam os trabalhadores, sejam elas diretamente empregadas ou como parte da força de trabalho, como no caso dos colaboradores terceirizados. Isso pode exigir a elaboração de medidas locais e dos processos. (COLWILL, 2010)

Abrindo o leque das dimensões de segurança informacional, vê-se que a questão educacional do colaborador e cidadão, no que tange à Segurança da Informação, deve ser pensada não apenas no âmbito empresarial, mas também no que se refere ao comportamento dessa pessoa fora da organização.

Dominar os riscos da informação através da segurança da informação poderia ajudar a reforçar a confiança no mercado eletrônico de trabalho. Não há verdadeiro obstáculo tecnológico para continuar o desenvolvimento de ações de segurança da informação, entretanto, no âmbito de aplicação e implantação de medidas de segurança

eficazes torna-se muito complexo e os custos relacionados não são menores. Parcerias público-privadas são desejáveis, tanto a nível nacional quanto internacional, com o objetivo de integrar segurança na infraestrutura, promover uma cultura de segurança, comportamento e ferramentas. Os recursos financeiros, processuais e organizacionais apoiariam a implantação efetiva de ações de segurança cujo benefício seria de todos (GHERNAOUTI-HELIE, 2009).

O desenvolvimento de uma cultura de segurança da informação é um dos meios para se elevar o nível de compreensão de cada membro da cadeia de segurança cibernética. Os esforços educacionais e investimentos precisam ser feitos para educar e treinar todos os membros da sociedade da informação: desde os tomadores de decisão, aos cidadãos, incluindo crianças e idosos. As ações específicas devem ser tomadas a nível nacional, para aumentar e construir capacidades de segurança cibernética de vários membros, e com isso desenvolver a capacidade de se lidar com uma ampla gama de questões a nível nacional e internacional (GHERNAOUTI-HELIE 2009).

A expectativa é que a formação do cidadão contribuirá para que este tenha uma atitude mais consciente frente a incidentes de segurança, independentemente do ambiente corporativo ou social. Conforme pontuado por Workmann (2007) que realizou uma leitura, em seu estudo, da teoria situacional de públicos, observou-se que um povo pode ser segmentado com base em sua atuação efetiva ou passividade do comportamento de comunicação. Esse ponto focal se desdobrou em componentes tais como o reconhecimento do problema, o nível de participação ativa e o reconhecimento de restrição. O reconhecimento do problema reflete na medida em que um indivíduo reconhece um problema como relevante para ele; isto é, qual a probabilidade de uma ameaça ser percebida como impacto para a pessoa. Com relação ao segundo componente - nível dos resultados da participação ativa - trata-se de uma percepção de como emocionalmente o problema é sentido, como a ameaça é percebida pelas pessoas como grave e/ou danosa. Já o reconhecimento de restrição reflete o grau em que as pessoas percebem seu comportamento como limitado por fatores além de seu próprio controle. Workmann complementa o referido estudo com as percepções de Grunig (1997) dizendo que, se estes três fatores descreverem com precisão as condições externas, ocorre, na sequência, uma mudança no ambiente antes da reação ou resposta por parte do cidadão. Entretanto, se ocorre internamente o ato de percepção, as ações e reações podem ser alteradas e, nesse caso, o instrumento promotor da mudança é a

comunicação persuasiva. Por isso o fator persuasão é determinante do comportamento das pessoas frente a situações de ameaça. Trabalhando possíveis desdobramentos frente à persuasão, detectaram-se três fatores emergentes: confiança, medo e compromisso.

Os autores Narita & Kitamura (2010) cruzam a questão da persuasão com a ação do que chamam de “Agentes Conversacionais”. Segundo os autores, esses agentes desempenharão um papel importante, porque eles podem interagir com os usuários através da conversa de uma forma pró-ativa. Durante as conversas convencionais agentes visam dialogar com os usuários enquanto eles podem, sem qualquer objetivo específico da conversa. Em contrapartida, os agentes persuasivos ou “agentes conversacionais” têm o claro objetivo de persuadir os usuários a mudar suas atitudes ou comportamentos. Não é admissível para agentes de persuasão deixar o *chat* no curso da natureza. Como persuasores humanos, mudam suas respostas dependendo do enunciado do adversário e da situação. Agentes persuasivos precisam de flexibilidade para interagir com os usuários e assim persuadi-los.

Vários ataques se concretizam quando invasores em potencial utilizam a aceitação de determinada mensagem junto ao usuário através de elementos tais como credibilidade, simpatia ou um atrativo qualquer no remetente da mensagem, ou seja, utilizam uma rota periférica de persuasão. Existem algumas características que são vinculadas à rota periférica de persuasão e podem ser descritas como:

- Reciprocidade. A reciprocidade está vinculada ao compromisso normativo no qual pessoas formam implícita obrigação de outros, ou seja, se algo de valor é oferecido, como uma amostra grátis, as pessoas sentem-se obrigadas a devolver o favor de fazer uma compra que não tinham previsto inicialmente.
- Consistência: teoricamente envolve compromisso de continuidade nos quais as pessoas se tornam psicologicamente investidas em uma decisão que outros tomaram.
- Prova Social: envolve o comprometimento afetivo, onde as pessoas tomam o modelo de comportamentos de seu grupo, de colegas, modelos, como importante demais, ou porque é geralmente "moda".

- Simpatia: pode ser usada para ganhar a confiança das pessoas. “Simpáticos” são percebidos como credíveis devido a conhecimentos especiais e/ou habilidades, tais como figuras do esporte ou atores etc.
- Autoridade: pode ser utilizada para gerar medo, onde as pessoas obedecem a comandos para evitar uma consequência negativa.
- Escassez: baseado no princípio da reatância, onde as pessoas respondem a percepção de faltas, dando maior valor psicológico sobre a percepção de itens escassos (WORKMANN, 2007).

Além da busca de sinais de comportamento adverso em potenciais invasores, a preocupação com ataques reais precisa sempre ser mantida. Isto deve envolver uma combinação de medidas processuais, de gestão de pessoas e desempenho em todos aqueles sob mandato de um gestor, incluindo os colaboradores terceiros. Isso deve levar a uma relação mais estreita entre os requisitos de segurança e do negócio como um todo. Acredita-se em uma abordagem ativa em detrimento da reativa em ambos os elementos – *gestor* e *colaborador* - e relatório individual para a mudança das circunstâncias. O foco não deve estar em apenas recolher diferentes itens de dados sobre o comportamento anômalo, mas também em coligir e analisar os dados para determinar os padrões e cursos de medidas corretivas (COLWILL, 2010).

O Rastreamento do esforço do usuário é importante e eficaz tanto na manutenção da segurança e na redução de atrito entre empregados e organizações, quanto entre a economia e os processos de segurança em uma organização.

Deve-se admitir que a ameaça à informação privilegiada e à segurança da informação não pode ser eliminada, mas pode ser controlada, avaliada e gerenciada. Através da compreensão dos fatores humanos vinculados à segurança informacional, consegue-se obter uma melhor compreensão dos riscos reais que as organizações enfrentam hoje no ambiente comercial global. A transformação organizacional, especialmente quando envolve o *outsourcing*, cria responsabilidades e uma mistura complexa de "ambientes hostis", além de um aumento no número de colaboradores com menores níveis de confiança e lealdade. Nenhuma organização existe em um vácuo e tampouco tem empregados apenas para o trabalho. Todo um contexto de mudança organizacional, ambiente cultural, tecnológico, social e econômico continuará a colocar demandas sobre as organizações de maneira a reavaliar o acesso às informações e

proteger seus ativos. Em tempos de crescente globalização, cuidados especiais devem ser tomados e, especialmente no que tange aos colaboradores terceirizados, restrições ao acesso às informações organizacionais devem ser impostas. Promover acesso apenas às informações que os terceiros precisam pelo período que eles precisam. A gestão informacional deve ser eficaz e o uso informacional deve ser controlado para que qualquer comportamento anormal seja investigado e ações de contenção sejam postas em prática (COLWILL, 2010).

Essa seção contribui para a construção do instrumento de coletas de dados quando delimita vários elementos que são determinantes para se garantir a segurança dos ativos informacionais corporativos e que não são contemplados na gestão de segurança informacional de várias organizações. A maioria desses elementos serão explorados no modelo que será proposto nessa pesquisa como fatores determinantes para o sucesso na gestão de segurança informacional.

As informações levantadas nessa seção e que farão parte do questionário são:

- Você entende o que é segurança da informação
- Você, dentro de suas atribuições e funções no dia-a-dia, se sente parte responsável pela segurança da informação praticada na instituição?
- A partir das diretrizes que a instituição fornece sobre como agir seguramente, eu consigo entender como atuar e agir de modo a garantir a confidencialidade, disponibilidade e a integralidade dos dados com os quais trabalho.
- Na minha percepção, a instituição investe mais em tecnologia para assegurar a segurança da informação corporativa e menos em treinamentos para as pessoas sobre segurança da informação e em políticas de segurança da informação.
- Eu poderia dizer que as ações de segurança da informação em minha instituição geram conhecimento e promovem o aprendizado entre os colaboradores?
- Frequentemente ocorrem interações sociais entre os colaboradores para discutir temas sobre segurança da informação.
- Você fica ciente de todas as atualizações de avaliação de riscos de seu departamento, setor ou área?

- Você sabe quem são as pessoas responsáveis pela segurança da informação na sua instituição?
- Conheço os procedimentos e políticas de segurança da informação adotadas pela instituição na qual trabalho.
- Costumo conversar com colegas sobre incidentes de segurança da informação ocorridos comigo ou que tenham ocorrido com eles ou com alguém que conheçamos.
- Tenho oportunidade de sugerir ações de segurança da informação na instituição na qual trabalho.
- Através das regras de segurança da informação disponibilizadas por minha organização, eu consigo entender qual deve ser o seu comportamento e como a empresa espera que eu aja com relação à segurança da informação.
- Posso dizer que há envolvimento e apoio das gerências, diretorias e presidência no que concerne às ações se segurança da informação.
- Posto em redes sociais fatos ou ocorrências que aconteceram na organização ou no meu setor para alertar amigos.
- Sinto vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é segurança da informação de minha instituição.
- Você poderia dizer que em primeiro lugar você dedica atenção à sua profissão e à especialidade do computador no qual trabalha para depois absorver os valores, missão e visão da empresa para a qual trabalha.
- Sou treinado para ter um comportamento seguro.
- Sei com clareza qual é o meu papel na segurança informacional da empresa.
- Existem, na instituição na qual trabalho, programas de educação para formar pessoas com relação à segurança da informação.
- As ameaças de segurança da informação que sofro determinam meu comportamento frente às situações que vivencio.
- Avaliando a situação atual, sinto que o ambiente da empresa é seguro no que concerne às informações que nele são processadas.

- A alta carga de trabalho vinculada à minha atividade prejudica minha percepção e ação com relação à segurança da informação.

3.2 - Segurança e Recursos Organizacionais

As organizações são compostas de uma série de elementos, dentre os quais se destacam os recursos humanos, os recursos físicos e virtuais e os processos, que combinados devem auferir a estas, otimização de tempo e de recursos, maior assertividade e ganhos de lucratividade.

Assim clientes, liderança, sociedade, estratégias e planos devem estar interligados com pessoas, tecnologia e processos na busca dos resultados esperados.

Os processos organizacionais têm tarefa de construir um alicerce entre os recursos disponíveis e os objetivos da empresa. Desta forma, quando se foca em segurança da informação organizacional, os controles formais, ou processos, serão os procedimentos e políticas adotados pela empresa para controlar o acesso e o uso da informação (SVEEN, TORRES **&** SARIEGI, 2009).

O objetivo dessa seção é entender como funcionam os controles formais no que concerne à segurança da informação e como os processos se inter-relacionam com tecnologia e pessoas.

3.2.1 Segurança da Informação e Processos – abordagem no contexto das políticas de informação

A informação é um ativo de grande valor nas relações mundiais contemporâneas. Por isso exige cuidado e preocupação da parte das empresas no que concerne à proteção desses ativos contra riscos e ameaças. Segundo Almeida (2007):

> Os problemas de muitas organizações na implementação de segurança da informação estão relacionados à dificuldade em definir o que deve ser protegido, qual o nível de proteção necessário, e quais as ferramentas utilizar no ambiente corporativo. A dificuldade começa na própria definição do objeto a proteger, ou seja, na definição da informação. Almeida (2007) *apud* Wilson (2002) alerta para o uso indistinto dos termos dado e informação. Para o autor, dados são fatos e estão fora da mente de uma pessoa.

> Informações consistem de dados aos quais se incorpora um contexto relevante para o indivíduo. Cabe então à organização descobrir em que contextos a informação critica se manifesta e as necessidades corporativas em relação à segurança, e não apenas buscar proteção para dados em computadores e em redes (ALMEIDA, 2007, p.1).

Um dos procedimentos usados com esse fim é a adoção de controles formais – políticas e procedimentos - cujo objetivo é garantir a segurança da informação e o correto desempenho dos outros dois tipos de controles - aqueles relativos às pessoas (informais) e os técnicos. A expectativa é de que, através dos controles formais, sejam reduzidos os índices de riscos e falhas, uma vez que trarão mais domínio e conscientização acerca da segurança informacional para os trabalhadores envolvidos em atividades de determinada empresa.

Nessa vertente, a própria definição de informação é pré-requisito para a acepção do conceito de políticas de informação e seu consequente desenvolvimento, cuja característica é ser multifacetada e plural (BROWNE, 1997 b; BRAMAN, 1989). Este quesito de pluralismo é flexível e se abre para uma gama de valores que apoia os formuladores de políticas no estabelecimento de decisões de nível cultural.

Diante do pluralismo, a hierarquia nas variações de escopo e complexidade aparece como elemento articulador de uma regra para formulação de decisão que permite classificar a diferenciação do poder dado à informação e suas categorias de criação, processo, fluxo e uso. Assim, a distinção acerca dessas dimensões promove definições de informação mais comumente usadas no processo de formulação de políticas e que podem ser agrupadas em: informação como recurso, como *commodity*, como padrão de percepção e como força constitutiva na sociedade (BRAMAN, 1989).

- Informação como recurso: é a informação que pode ser processada e que possui valor de ativo, uma vez que dá suporte ao desenvolvimento social e organizacional. Nesse conceito, a informação, seus respectivos criadores, processadores e usuários são vistos como entidades discretas e isoladas.
- Informação como *commodity*: esse tipo de informação é aquela que pode ser comprada e vendida e que ganha valor à medida que perpassa a cadeia produtiva empresarial. Esse

conceito exclui a maior parte das abordagens de informação cultural, religiosa e de estética significante.

- Informação como percepção: este conceito reconhece que padrões e contextos são variáveis distintas entre os indivíduos e devido a isso a informação adquire o caráter de relatividade. Nessa abordagem é possível aproximar a informação dos fenômenos de subjetividade e intangibilidade e tratar os efeitos da informação, como redução de incertezas.
- Informação como força constitutiva na sociedade: trata-se de um conceito de informação que tem poder tanto pela legitimidade e própria razão de existir quanto tem poder para moldar o contexto. Acredita-se que essa dimensão proposta deva ser a base para as políticas de informação, entretanto deve-se reconhecer que esta ferramenta pode ser usada para manipulação ideológica (BRAMAN, 1989; BROWNE, 1997).

Uma visão complementar sobre informação, especificamente no campo dos negócios, é a apontada por Cendón (2003) na qual a autora coloca que a informação é um dos principais insumos para tomada de decisão, haja vista que reduz incertezas, monitora a concorrência, identifica ameaças e oportunidades e melhora a competitividade.

Nesse âmbito, percebe-se que um programa de segurança informacional que abarque a totalidade da empresa demanda um entendimento claro do tipo e escopo de informação da qual a organização está tratando, para que as ações de segurança da informação sejam desenvolvidas em linha com esse conceito. A proposta é que seja delimitado desde o início do processo de desenvolvimento de ações de segurança informacional um entendimento da parte de todos os elementos corporativos, principalmente dos recursos humanos, sobre qual informação no ambiente organizacional que deve ser considerada como ativo.

Esta delimitação é essencial e prioritária, uma vez que a incorreta demarcação do ativo informação pode gerar lacunas por abarcar um grande volume de elementos comprometendo a efetividade, o controle e a eficiência das ações e,

consequentemente, demandando muito mais esforço para classificar as informações que devem ser protegidas.

No caso desse estudo, a fixação da definição de informação que norteará as ações terá como suporte os conceitos de informação como recurso e de informação como força constitutiva na sociedade. Acredita-se que o mix dessas conceituações trará a amplitude e o arcabouço necessário para apoiar as propostas. Caberia também nessa pesquisa considerar a informação no âmbito da percepção, entretanto entende-se que a proposta da informação como força constitutiva na sociedade inclui de alguma forma características da informação como percepção, primordialmente a ênfase no elemento contexto como diferenciador da percepção de informação entre os indivíduos que compõem a sociedade que é abordada nas duas vertentes. Inclui-se nessa abordagem a perspectiva apontada por Céndon (2003) que trará contribuição da informação no âmbito dos negócios.

Assim, trabalhar a segurança da informação no âmbito dos processos traz à discussão um elemento acionador que são as políticas de informação e. consequentemente, as políticas de segurança da informação. As políticas aparecem como componente articulador e chave na condução e definição dos processos, norteando as ações a partir de sua concepção e desenvolvimento.

Desta forma, é preponderante trazer à luz dessa discussão o conceito de políticas de modo que sua concepção aliada à definição de informação possa direcionar o desenvolvimento do escopo das políticas de segurança da informação de forma sustentável.

O termo política, segundo Browne (1997), refere-se a estratégias usadas no setor público-privado para garantir suporte informacional e cumprimento de objetivos, além de promover o crescimento da competitividade e da eficiência. É comum nos depararmos com situações nas quais um programa de ações informacionais planejado para construir a cultura corporativa de uma instituição seja descrito como uma política. Por isso, deve-se estar atento ao fato de que uma política organizacional deve ser desenvolvida de forma flexível, ampla e de modo que faça a interlocução entre as influências advindas das políticas públicas e as demandas e necessidades da política privada.

Desta forma, a busca por definições acerca do que vem a ser política aponta como solução abordagens pragmáticas usadas na área da ciência da informação. Propõe-

se abaixo um recorte dentre as inúmeras abordagens existentes acerca do tema. Segundo Browne (1997), são elas:

- Política como teoria ou modelo: o uso da política envolve aspirações acerca do que se pode e do que não se pode fazer e as respectivas consequências. Entretanto, as políticas não podem ser expressas ou expressar um modelo de causa-efeito. Os modelos normalmente divulgam os tipos de desenvolvimento e de implementação de políticas predominantes no contexto daquela sociedade ou país;
- Política como expressão de um propósito geral ou estado desejado das coisas: este propósito foca massiçamente na retórica em detrimento da realidade e resgata a política como sendo o mérito pelo desempenho de uma atividade ou estado desejado das coisas caso os objetivos sejam cumpridos. Muitos dos elementos que categorizam a explosão da informação se enquadram nessa categoria. Na versão americana encontram-se presentes os seguintes elementos: promover recursos para encontrar as demandas dos consumidores, aumentar a produtividade, impulsionar a inovação, melhorar a qualidade de vida, criar comunidades de interesse, robustecer a educação, melhorar a saúde, aumentar as opções de lazer e reforçar a democracia participativa;
- Política como rótulo para determinada atividade: nesse escopo diferentes declarações são desenvolvidas em diversas esferas políticas, como a política internacional, a política econômica etc., cujo foco é na atividade governamental. Essa proposta interage nos domínios nacionais e regionais das políticas de informação.
- Políticas enquanto decisões governamentais: as decisões governamentais são comumente delineadas como políticas, ainda que não sejam promovidas a ações previstas na

legislação. Um exemplo é o caso da Inglaterra que debatia o conceito de "informação negociável". A proposta é que a informação em poder do estado seja disponibilizada para o setor privado de modo que ela seja usada no desenvolvimento de informações eletrônicas;

- Política como proposta específica: trata-se de declarações de atividade e direções que interessam a grupos que precisam seguir deliberações governamentais.
- Política como processo: a ideia de olhar a política como um processo é dominante na esfera pública. Entretanto, existem críticas a algumas abordagens que tratam diferentes fases como sequenciais e independentes uma da outra por um período (BROWNE, 1997).

Entender e delinear dentre os conceitos de política aqueles que conduzirão à definição das políticas de segurança da informação é fator preponderante para o andamento dos trabalhos. Dentre as propostas aqui destacadas, observa-se uma sinergia entre a política e o setor governamental, entretanto, para o estudo em questão, a proposta é que se destaque o conceito na perspectiva corporativa. Diante disso, a análise das propostas leva a considerar como melhor alternativa para o estudo a definição de política no âmbito da expressão de um propósito geral ou estado desejado das coisas. Acredita-se que essa perspectiva venha dar suporte à proposta de visão da segurança da informação como um processo de melhoria contínua.

Paralelamente, a perspectiva de se desenvolver uma política de segurança da informação, que tenha como base a expressão de um propósito geral ou estado desejado das coisas, permite que os componentes da organização tenham clareza acerca das delimitações e propósitos que regerão a política de segurança da informação. Assim, no caso de "estado desejado das coisas", podem-se desenvolver ações no sentido de pautar o comportamento desejado do colaborador no que concerne à segurança da informação, tanto no que diz respeito à conduta, à cooperação, quanto à comunicação de incidentes de segurança, fato este que envolve diretamente a aprendizagem organizacional.

Integrando os conceitos de políticas e de informação, Braman (1989) pontua que as políticas de informação serão direcionadas conforme as divisões políticas de

classe, a sócioeconômica e as diferenciações qualitativas no que diz respeito ao fenômeno *informação*, nos diversos níveis da sociedade. Por isso, salienta-se que as políticas de informação devem seguir uma hierarquia de definições para consequente escolha daquelas que sejam coniventes à situação ou ao uso proposto.

De fato, na sociedade contemporânea as organizações interagem com um fluxo constante e cada vez maior de informações. Para executar essa tarefa contam com uma série de ferramentas, técnicas, procedimentos e com o aparato tecnológico desenvolvido pela Tecnologia da Informação.

Nesse aspecto observa-se que, no caso do determinismo tecnológico, a conjectura histórica é fator peremptório dos desejos da população, e esses desejos são expressos na formulação e implementação de suas políticas. Essas políticas são ações para definir as direções de mudança. Assim, a Política de Informação é um termo de uso geral percebido nas arenas de tomadas de decisão e pelos *players*, e vem se tornando um lugar em comum no qual muitas das mesmas questões desde o *design* de processos até a privacidade dos dados surgem como temas. As categorias que cada indivíduo da sociedade utiliza para definir informação formarão um quadro que servirá de base para ajudar no desenvolvimento das políticas de informação. Paralelamente, os formuladores de políticas, tanto públicas quanto privadas, nos Estados Unidos, argumentam a favor da perspectiva econômica como direcionadora das discussões sobre o fluxo de informação internacional, especificamente porque promove um meio de se distinguir a questão social da questão econômica, permitindo aos formuladores de políticas que excluam interesses sociais, políticos ou culturais quando negociarem com o que preferem ver como problemas puramente econômicos (BRAMAN, 1989).

Integrando os conceitos de políticas e de informação no viés empresarial, Rowlands (1996) coloca que as políticas de informação nesse contexto são aquelas orientadas à aplicação e buscam determinar a maneira mais eficiente de lidar com um problema particular. Esta abordagem foca a realização de uma meta com a qual a política de informação se compromete e reforça que esse objetivo não pode ser alcançado sem referência a uma ideologia ou uma posição normativa.

Fazendo uma relação dos autores citados no que concerne aos conceitos de informação, políticas e políticas de informação, observa-se que nas abordagens escolhidas para este estudo há uma convergência dos conceitos de informação e política culminando no conceito de políticas de informação. Ao unir as abordagens de

informação como um ativo, somado ao conceito de política como expressão de um propósito geral ou estado desejado das coisas, há uma definição política de informação que integra essas duas perspectivas, haja vista que propõe foco em uma meta através de uma perspectiva orientada à aplicação, ou seja, à política aplicada.

Consegue-se, através dos aspectos apontados, ter uma base para sustentar e delinear as políticas de informação de uma organização. Essa perspectiva é importante porque esse direcionamento inicial ajudará na formação dos pilares que sustentarão a política de informação da empresa e essa perspectiva influenciará a maneira pela qual a política de informação será desenvolvida.

Assim, trazer à luz dessa discussão as perspectivas que envolvem o elemento informação e o elemento políticas é de fundamental importância para contextualizar a abordagem de processos como elemento integrador da gestão de segurança informacional corporativa. Mesmo porque, quando se fala sobre políticas de informação, observa-se que seu escopo recebe a mesma perspectiva delineada à informação, ou seja, o pluralismo e as multifacetas. Desta forma, versar sobre Segurança da Informação implica em aceitar que o referido termo pode ter vários significados, dependendo do enfoque que é dado e do contexto no qual é empregado.

Todas as questões e abordagens pertinentes à Segurança da Informação merecem especial reflexão, principalmente por que a demanda da sociedade é por soluções que interajam e integrem todo o contexto organizacional. Desta forma é necessário, conforme apontado por Wylder (2004), desenvolver políticas, processos e procedimentos de segurança informacional que tenham como suporte um programa de segurança informacional e contemplem todos os níveis da organização, haja vista que o processamento de informações ocorre em toda a estrutura da empresa e envolve tanto elementos técnicos e processuais quanto humanos da composição organizacional.

Em geral, o sucesso da gestão dos processos de segurança informacional e das políticas de segurança da informação adotada por uma instituição depende da combinação de diversos elementos, dentre eles: a estrutura organizacional da empresa; as normas e os procedimentos relacionados à segurança da informação e a maneira pela qual são implantados e monitorados; os sistemas tecnológicos utilizados; os mecanismos de controle desenvolvidos; assim como o comportamento de diretores, funcionários e colaboradores (BMF BOVESPA, 2011).

Devido a esse complexo sistema, nota-se que várias empresas resumem a existência de gestão de segurança informacional às políticas de informação e elas são apresentadas e apontadas como o mecanismo ratificador da existência de segurança da informação naquela corporação. Merece destaque a presença do elemento humano como agente que usará os processos e as políticas de informação organizacionais como direcionadoras do seu comportamento na organização.

A Política de Segurança da Informação é um dos pilares da gestão de segurança informacional e fornece apoio, na perspectiva formal, à gestão de segurança da informação (DA VEIGA **&** ELOFF, 2010).

Segundo Almeida (2007, p.156), uma política de segurança é um plano de alto nível que estabelece como a segurança deve ser praticada e qual nível de segurança – com custos e benefícios inerentes – a organização está disposta a aceitar.

A política de segurança da informação é caracterizada como um controle formal que inclui procedimentos que controlam o acesso e uso da informação, com o objetivo de estabelecer e assegurar o uso eficaz de controles técnicos, além de fornecer apoio a todas as ações de segurança informacional. Pode-se considerar que os controles formais incluem auditorias de sistema, atualização de mecanismos de avaliação de riscos, identificação de papéis de segurança, a segregação de responsabilidades, aplicação de indicadores, além de necessitarem de mais tempo de implementação e execução (SVEEN, TORRES **&** SARIEGI, 2009).

Os controles técnicos dependem de controles formais para garantir a plenitude de sua funcionalidade. Por exemplo, a proteção por senha é inútil se a senha está escrita em uma nota que está presa ao monitor. Senha de controle de acesso é uma medida técnica e a senha presa ao monitor é uma violação de controles formais. Sugere-se que as instruções formais sejam disponibilizadas em um local para orientar os usuários sobre comportamento seguro e adequado. Sem tais instruções, ocorre uma falta de conscientização do usuário e estes não podem ser responsabilizados por uma violação de segurança, uma vez que a falta de controles formais é a verdadeira razão para violação. No entanto, se há instruções formais em vigor e a falta entendimento do usuário sobre o porquê uma senha não deve estar presa a um monitor (um controle informal) ocorre outra violação. Assim, quando um dos controles é posto em cheque, o erro se propaga sobre os outros controles (SVEEN, TORRES **&** SARIEGI, 2009).

Quando se cruza a perspectiva da segurança da informação com o fator humano, observa-se que erros humanos podem estar relacionados a fatores organizacionais como comunicação, cultura, segurança e políticas. Especificamente, vê-se que erros na fase de processamento da informação constituem a maioria dos casos de violações de privacidade relacionadas a erros humanos. Já na área da política, houve uma série de fatores que poderiam contribuir para uma política de segurança ineficaz e, inclui-se neste caso, a falta de especificação, documentação, falta de capacidade interna de criar políticas efetivas e uma falta de responsabilidade ou mecanismo de execução para fazer cumprir a política (KRAEMER, CARAYON **&** CLEM, 2009).

Outra deficiência grave é que grande parte das empresas estão atrasadas na evolução do ambiente de ameaças. Novas vulnerabilidades são descobertas de forma contínua e é preciso tempo para implementar controles de segurança. Este delta de tempo de espera pode permitir a ocorrência de um ataque antes da implementação dos referidos controles de segurança (SVEEN, TORRES **&** SARIEGI, 2009).

O fato é que a implementação eficaz de uma política de segurança é essencial: mesmo embora a maioria das empresas tenha políticas, apenas uma minoria parece aplicá-las. As organizações necessitam estabelecer regras claras e coerentes para o que se espera de seus especialistas e colaboradores. Uma abordagem é reforçar as políticas de rigor e proibir qualquer uso pessoal dos ativos da empresa no local de trabalho. Embora esta ação venha a implicar no bloqueio de redes para todos, o propósito é obter controle de acesso rigoroso para sites não relacionados ao trabalho, garantir o cumprimento legal, evitar o desperdício de tempo e riscos de infecções por *malware*. Atenção deve ser dada à aplicabilidade de um controle rigoroso e auditoria a todas as formas de acesso aos ativos físicos e lógicos da empresa (COLWILL, 2010).

As avaliações de risco podem fornecer uma base para a contínua melhoria. Elas devem ser realizadas em intervalos regulares e cuidados devem ser tomados para aprender o máximo possível com elas. Os resultados da avaliação de risco fornecem uma base para seleção e implementação de controles de segurança, mas também servem como fatores importantes para a avaliação de risco seguinte. Outros benefícios podem ser computados, tais como: transferência de conhecimento da equipe de avaliação de risco para o pessoal da empresa; aumento da comunicação sobre questões de segurança entre unidades de negócios (segurança é multidisciplinar e potencialmente toca todas as

unidades de negócios de uma empresa); e, maior sensibilização para a segurança dentro da empresa (SVEEN, TORRES **&** SARIEGI, 2009).

O processo de definição de objetivos no âmbito sistemas de gestão de segurança da informação poderia ser mais eficiente se contasse com a participação dos trabalhadores em atividades de grupo e os conhecimentos sobre questões de segurança fossem igualmente compartilhados entre os funcionários através de atividades chave de participação (KOSKOSAS, CHARITOUDI **&** LOUTA, 2008).

Através do mecanismo de aprendizagem a percepção de segurança, por exemplo, em uma avaliação de risco, aumenta. O corpo de conhecimento em segurança da informação da empresa aumenta e este fato reforça a percepção para detectar falhas de segurança. Doravante, sugere-se que rotinas e instruções estejam disponíveis em local acessível para identificar os incidentes que ocorrem devido à falta ou ineficácia dos controles (SVEEN, TORRES **&** SARIEGI, 2009).

Os controles de segurança devem ser ágeis e terem possibilidade de ser praticados em uma variedade de ambientes e, preferencialmente, ser desenvolvido com a participação do usuário final. A tecnologia pode fornecer um meio para controlar o acesso a informações e ajudar no controle e detecção de programas maliciosos, mas são o ambiente de trabalho e os fatores humanos que irão fornecer as bases reais para o sucesso. As mudanças devem ser apoiadas pela educação contínua e sensibilização. Em termos de controles de atenuação, a tecnologia não deve ser considerada em isolamento: se as pessoas não cooperam em compreender a razão para os controles de segurança, eles podem encontrar uma causa e meios para subverter ou contornar as restrições técnicas que lhes são impostas, sobretudo quando a contrapartida é uma recompensa (COLWILL, 2010)

Uma abordagem complementar é exposta por Da Veiga **&** Eloff (2010) quando relatam que as organizações devem garantir que a interação dos funcionários esteja em consonância com os requisitos da política de segurança da informação. Estes requisitos relacionam-se com ações, tais como a realização de back-ups para o servidor em uma base diária, uso de senha para proteger as informações sobre mídia removível ou a supressão de correio eletrônico com anexos não solicitados.

Efetivamente quando se investiga a absorção, o conteúdo, a difusão e o impacto das políticas de Segurança da Informação, observa-se que alguns fatores são percebidos como mais importantes: compromisso visível de gestão; boa compreensão

dos riscos e requisitos de segurança; distribuição e orientação das políticas de segurança; apoio da alta gerência e compartilhamento de conhecimento (KRAEMER, CARAYON **&** CLEM, 2009).

Apesar das necessidades constatadas acima, ainda há ocorrências, em algumas empresas, de não cumprimento de políticas de segurança. Uma investigação conduzida por Beautement **&** Sasse (2009) relata que decisões foram tomadas, em grande parte, com base na avaliação do custo e benefício dos indivíduos envolvidos no cumprimento de políticas de segurança. Quando os participantes eram conscientes do risco específico e que a política foi atenuante, eles eram mais propensos a cumprir. Entretanto, quando eles decidiram não cumprir, esses participantes justificavam sua conduta em termos do impacto negativo das políticas de segurança na produtividade da organização (por exemplo, uma perda de venda, porque eles não podiam acessar o sistema e produzir uma simulação em tempo) ou, sobre o impacto que essas políticas tiveram sobre eles pessoalmente (por exemplo, a luta para lembrar senhas). Os empregados pesaram a percepção da necessidade de uma política de segurança específica contra a percepção do esforço necessário para cumprir com esta política.

Uma vez que estas decisões influenciam comportamento de aderência, decidiu-se cruzar informações e explorar as contribuições dos gestores de segurança nesse cenário. Observou-se que, na maioria das organizações de hoje, a carga de trabalho associada a políticas de segurança é delegada para os funcionários. Entretanto, os gerentes de segurança precisam saber a quantidade de diretrizes e normas com que um grupo de colaboradores está lidando e o esforço de cada grupo em cumprir essas determinações.

Recentemente, explicações de recomendação estão se tornando um tema relevante para melhorar o desempenho de recomendação e a capacidade de persuasão é um elemento chave das explicações para convencer os clientes a selecionar um item, ou colaboradores a ter determinado tipo de comportamento (NARITA **&** KITAMURA, 2010).

Ao se analisar a questão através do macro ambiente organizacional, percebe-se que segurança, educação e programas de sensibilização devem ter como objetivo aumentar os níveis de confiança entre empregador e empregado, através do desenvolvimento de uma compreensão das razões para as políticas segurança e aplicação de controles, bem como o fato de este ser um interesse de longo prazo de

todos os membros da organização. Educação sobre reais ameaças e vulnerabilidades de segurança são necessárias, por exemplo, sobre o uso de fontes não confiáveis, dispositivos e outros computadores que são tidos como práticas inseguras. Pessoas conscientes estão mais propensas a reconhecer e relatar qualquer atividade suspeita. O aumento da sensibilização dos funcionários provavelmente promova a redução da probabilidade de violação acidental e aumente a possibilidade de ser detectada e comunicada uma atividade maliciosa. Da parte da organização, todo esforço necessita ser feito para garantir que colaboradores não aleguem ignorância das regras. Programas de conscientização são essenciais em ambientes com grandes volumes de negócios e de pessoal, apesar de que medir o sucesso de tais programas possa ser difícil.

Um fator chave e direcionador do sucesso é a implantação dos controles de segurança (incluindo o acompanhamento de funcionários e associados e sanções políticas) proporcionais aos potenciais riscos envolvidos. Bom comportamento de segurança deve ser reforçado e recompensado. Algumas organizações enfatizam que o acompanhamento pode realmente beneficiar o pessoal, uma vez que os funcionários estão convencidos de que a empresa na qual trabalham protege contra vazamento os ativos informacionais e, portanto, contra possíveis danos à sua reputação ou saúde financeira, além de proteger contra acusações indevidas, podendo proteger os empregos (COLWILL, 2010).

Essa seção contribui para a construção do instrumento de coleta de dados quando delimita que as políticas são veículos cruciais na gestão de segurança das informações corporativas, uma vez que elas delimitam a forma que a organização deseja que seus colaboradores atuem e, como os recursos físicos e virtuais podem e devem ser processados e administrados. Através desse levantamento consegue-se descrever quais variáveis podem ser exploradas na gestão de segurança das informações corporativas para se garantir a confidencialidade, integridade, disponibilidade dos dados e informações, e, paralelamente os controles para uso e acesso da informação e sua interrelação com os elementos tecnologia e pessoas.

As informações levantadas que se transformaram em questões no instrumento de coleta de dados são:

- Percebo que a instituição empreende e explora as ações de segurança da informação para, através delas, promover a melhoria continua dos processos institucionais.

- Eu poderia dizer que a segurança da informação na instituição na qual trabalho faz parte do planejamento estratégico ou da gestão estratégica da empresa.
- Quando ocorre um incidente de segurança da informação na instituição, esse incidente é detectado, prevenido e documentado.
- Estão claras as condutas que a instituição deseja que eu tenha com relação à segurança da informação? Como exemplo podemos citar a comunicação de incidentes de segurança.
- Há ocorrência de auditorias sobre segurança da informação no seu departamento ou setor ou área?
- Há instruções e políticas formais em sua instituição que ensinam como a empresa espera que você aja com relação à segurança da informação.
- Há indicadores de segurança da informação que são avaliados pela instituição na qual trabalho.
- Há indicadores de segurança da informação que são avaliados pelo setor / departamento no qual trabalho.
- A instituição comunica aos colaboradores sobre os incidentes de segurança da informação ocorridos.
- Posso identificar as atuais medidas que estão sendo tomadas em relação à segurança informacional na instituição na qual trabalho.
- As especificações das políticas de segurança da informação da instituição na qual trabalho são de fácil compreensão.
- Os riscos, ameaças e vulnerabilidades com relação à segurança da informação de minha organização são bem documentados.
- Os riscos, ameaças e vulnerabilidades com relação à segurança das informações da organização na qual trabalho são devidamente comunicados aos colaboradores.
- Analisando as políticas de informação da organização na qual trabalho, eu diria que elas são efetivas e suficientes para garantir a confidencialidade, integridade e disponibilidade das informações (principalmente das informações sigilosas).

- Na minha instituição existem mecanismos de execução que propiciam o cumprimento das políticas de segurança da informação pelos colaboradores.
- No ambiente institucional posso escolher quais itens das políticas de segurança da informação vou cumprir.
- Considero volumosa demais a quantidade de diretrizes, normas e procedimentos que devo cumprir.
- Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação propostas pela instituição.

3.3– A Segurança da Informação e os Sistemas

Conforme discutido anteriormente, observa-se que a necessidade de proteção dos ativos informacionais das empresas faz com que a tecnologia ganhe uma posição de destaque nesse contexto globalizado. Entretanto, para este estudo, parte-se do pressuposto de que a tecnologia usada isoladamente não promoverá uma gestão de segurança da informação que abarque a totalidade da organização e tampouco assegure, isoladamente, a redução de custos financeiros, de perda de informação sensível, de competitividade, de ameaças, de vulnerabilidades e riscos inerentes à ocorrência de incidentes de segurança, principalmente quando estes envolvem seres humanos.

Portanto, essa seção traz uma contribuição para a análise do problema dessa pesquisa, uma vez que abordará os aspectos tecnológicos da segurança da informação com um olhar focado na inter-relação entre os aspectos técnicos, o elemento humano e a segurança da informação para descobrir como falhas de segurança são geradas a partir da interação entre a tecnologia e os seres humanos.

3.3.1 Segurança da Informação e Tecnologia – perspectivas de discussão no contexto da Ciência da Informação

No âmbito e na variedade dos sistemas de informação é que a informação é processada no ambiente organizacional.

O propósito de um sistema de informação, segundo Buckland (1991), é esclarecer os questionamentos que venham a surgir e despertar a curiosidade. Um sistema de informação é um recurso para a investigação e um veículo para procurar informar pessoas sobre determinado assunto. Por esse motivo, um sistema de informação é proposital. Dependendo do valor de cada usuário, pode-se concordar ou discordar com um determinado propósito, mas os serviços de informações são baseados em um tipo de escopo mesmo que eles sejam caracterizados como partidários, altruístas, frívolos ou ineficazes. A característica de uma gestão eficaz de um sistema de informação é o esforço contínuo para tornar os recursos de informação disponíveis no momento e no local nos quais forem necessários.

Nesse sentido, é importante destacar que a necessidade e uso da informação são determinados pelo usuário e ele utiliza os sistemas de informação para satisfazer suas necessidades informacionais. O ato de informar, segundo Allen (1996), envolve tanto uma atividade realizada quanto um processo vivenciado por alguém. Sendo que, na perspectiva do usuário, a informação é algo que acontece com este usuário, ou seja, pessoas se informam ou informam alguém.

Complementar a essa abordagem, destaca-se a contribuição de Ingwersen (1992) que coloca que o conceito de informação deve incluir o processo no qual o conhecimento do informante é transformado pelo ato da comunicação e, da parte de quem busca a informação, o conhecimento é transformado pelo processo de percepção, avaliação, interpretação e aprendizado.

As duas perspectivas apontadas são arcabouço para discutir a definição de sistemas de informação apontada pelos dois autores Buckland (1991) e Allen (1996). O primeiro aponta que os sistemas de informação usados por seres humanos são sistemas abertos e complexos, que interagem com outros sistemas de informação ao redor do mundo. Adicionalmente, outro aspecto importante e relevante é o fato desses sistemas terem habilidade de responder a mudanças, de adaptar seus ambientes e manter a estabilidade para sobreviver. Já o segundo autor destaca os sistemas de informação

como a junção de um ou mais dispositivos de informação que promovem acesso a um ou mais repositórios de conhecimento, além de se constituírem de ações através de mecanismos nos quais pessoas podem informar outras ou se informarem.

Efetivamente, trata-se de definições complementares, uma vez que apontam abordagens concernentes ao ambiente e seu dinamismo no mundo globalizado, aos usuários, suas necessidades e possibilidade de acesso a informações através das tecnologias num curto espaço de tempo e, por último, às informações que se confirmam como ativo de valor, sendo artefato de busca dos usuários e item de ação por parte das tecnologias.

Complementar a essa visão, Marchionini (1998) ressalta que infraestruturas de informação se desenvolvem à medida que os usuários da informação ganham conhecimento acerca dos fatores condutores da busca de informações e também das habilidades para gerenciar esse processo de busca informacional. Desta forma, entender qual o conhecimento e as habilidades necessárias em ambientes manuais e eletrônicos levarão a melhores *designs* para futuros sistemas de informação e melhores treinamentos, tanto para profissionais quanto para usuários.

As reflexões sobre o elemento *sistemas de informação* e as variantes que o compõem apontam para o paradigma da tecnologia da informação que contextualiza a sociedade da informação e as empresas como parte da sociedade, sob a perspectiva tecnológica. Nesse sentido, Castells (1999) aponta que as tecnologias são desenvolvidas para agir sobre a informação e que essa informação é elemento presente tanto no contexto coletivo quanto individual, sendo moldado pelo novo meio tecnológico. Esse novo meio tecnológico traz consigo a lógica das redes como fator unificador de sistemas ou conjunto de relações, sendo preponderantemente flexível. Essa característica de flexibilidade e sistematização em redes propicia a convergência das tecnologias para um sistema integrado e global.

As características de flexibilidade e de integração das informações em sistemas globais apontam para uma mudança de costume dos indivíduos. As pessoas demandam por tecnologias e essas tecnologias passam a ficar cada vez mais presentes na vida dos cidadãos. Nesse sentido, as novas tecnologias vêm mudando as atitudes sociais, tornando os dados e comunicações móveis cada vez mais disponíveis e de fácil uso.

Por isso, é importante entender o conceito de tecnologia da informação. A técnica denota o caminho de como fazer algo e a tecnologia pode ser descrita como o recurso físico que serve como ferramenta para realizar algo. Assim, as tecnologias da informação podem ser delineadas como aquelas utilizadas para "manejar" a informação. (BUCKLAND, 1991).

Mediada pela tecnologia e pela integração global dos sistemas de informação, pedidos de participação social se tornam cada vez mais populares e mais acessíveis, principalmente através de telefones celulares e outros dispositivos móveis. Esta participação social se dá por intermédio da rede e através de instrumentos como, por exemplo, *blogs, facebook, twitter, youtube*, *sites* de conteúdo em geral, grupos de discussão, relatórios de problemas, sistemas de recomendação, etc. (COLWILL, 2010). A intimidade da relação entre tecnologia e sociedade promoveu a possibilidade dos valores tecnológicos serem classificados como prioridades nacionais em praticamente todo o mundo, equiparadas com as necessidades de saúde, educação, energia, proteção ambiental e outras (PREECE, 2010).

A mudança global que transformou os padrões da sociedade através da união dos elementos *tecnologia* e *informação* mudou o "jeito de viver" das pessoas. Através das tecnologias da informação os cidadãos rompem fronteiras, trocam informações e adquirem conhecimento a uma velocidade inimaginável.

O vasto potencial da tecnologia para explorar oportunidades no que concerne às relações e estruturas sociais que impactam o indivíduo, tanto no ambiente de trabalho quanto em casa. Observa-se uma fusão de sistemas e aplicativos que são usados tanto em casa quanto no trabalho, gerando, por parte dos trabalhadores, requisição de maior liberdade de escolha para utilizar ferramentas de tecnologia da informação de acordo com suas preferências e com a prerrogativa de que assim realizarão um trabalho mais eficaz. Esta mão de obra, cada vez mais dependente das tecnologias da informação e da comunicação, não está longe de desafiar a gestão de segurança praticada, atualmente, nas organizações (COLWILL, 2010).

Cendón (2003) ressalta que as novas tecnologias não só permitem maior flexibilidade de se obterem dados atualizados, como também oferecem ao usuário maior flexibilidade na busca e na manipulação dos dados, haja vista a facilidade de acesso à informação propiciada pelo armazenamento dos dados em rede.

A presença marcante das diversas tecnologias em diversas áreas, das redes e das redes sociais na vida em sociedade, projeta a tecnologia a um lugar de destaque nas relações mundiais. A intimidade e a interação entre esses atores se consolidam a cada dia quando as pessoas acompanham o desenvolvimento tecnológico interagindo e necessitando de tais ferramentas em seus ambientes de convivência.

A totalidade desta conjuntura faz perceber a incontestável relação entre tecnologia e sociedade. Entretanto, é respeitável perceber, através da análise pela ótica dos recursos humanos no âmbito dos sistemas, redes e tecnologias da informação, que a tecnologia é projetada uma vez que é implementada e operada por pessoas. Assim, é o fator humano que determina as formas como usamos sistemas de informação ou o uso indevido destes (LACEY, 2009).

O produto dessas relações de interação – dados, informação e conhecimento, cujos valores despertam a necessidade de proteção por parte de quem as detém, no caso das empresas adquirem caráter de ativos e necessitam ser salvaguardadas de modo que venha a avalizar o aumento da competitividade, a redução de riscos, de ameaças, de vulnerabilidades, de custos financeiros e de perda de informação sensível.

A influência mútua dessas variáveis evidencia o quão complexos são os sistemas presentes nesse contexto, uma vez que tecnologia, pessoas e processos coexistem. Proteger os sistemas de informação é uma tarefa difícil que exige a implementação de três tipos de controles de segurança: controles técnicos (tecnologia), controles formais (processos) e controles informais (pessoas). Essa trindade de controles de segurança é necessária para atingir desempenho de alta segurança, especialmente porque estes são hierarquicamente dependentes uns dos outros e uma falha em um dos tipos de controles pode abrir brechas num outro (SVEEN, TORRES **&** SARIEGI 2009).

Apesar de sua direta dependência com os demais tipos de controles – formal e informal, nessa fase do estudo abordar-se-á diretamente apenas os controles técnicos.

Os autores SVEEN, TORRES **&** SARIEGI (2009) esclarecem que controles técnicos são ferramentas de hardware e software, tais como dispositivos biométricos, bloqueios, software antivírus, firewalls etc. que restringem o acesso a prédios, sistemas de computador, programas e etc. a fim de evitar seu uso indevido. Já Colwill (2010) contribui trazendo uma especificação dos controles técnicos contra invasores não somente externos, mas também internos à empresa, e diz que estes devem incluir,

minimamente, criptografia, controle de acesso, privilégio mínimo, acompanhamento, auditoria e relatórios. Já os autores KRAEMER, CARAYON **&** CLEM (2009) enfatizam a utilização de métodos específicos de segurança da informação, como os *smart cards*, dispositivos biométricos, software de criptografia PGP 5.0, senhas, segurança nos navegadores *web* básico, indicadores de identificação, análise das aplicações de desktop, tais como o *Word 2007 e Internet Explorer*.

Analogamente, faz-se notar que os sistemas de segurança da informação são desenvolvidos visando minimizar riscos decorrentes de acesso não autorizado e posse de informação e, nessa perspectiva na qual o ativo são os dados, a estratégia é garantir às bases de dados segurança através dos critérios de integridade, confidencialidade e autenticidade (KOSKOSAS, CHARITOUDI **&** LOUTA, 2008).

Hoje em dia, as pessoas usufruem dos benefícios do uso de computadores e da Internet para a comunicação e para fazer negócios. Por isso, o problema da segurança da informação está se tornando cada vez mais relevante. Para um computador comum e usuários da Internet, segurança da informação pode significar poder trabalhar com os computadores sem serem atacados por vírus, ser capaz de conduzir os negócios on-line sem se preocupar se seu número de cartão de crédito será roubado, ser capaz de ler e-mails sem receber spam, ou ser capaz de falar com amigos através do software de mensagens instantâneas sem se preocupar se a informação será grampeada. Assim, do ponto de vista técnico, segurança da informação é definida como ato de proteger a disponibilidade, exatidão, autenticidade, confidencialidade, utilidade, a integridade e a posse de informações (Whitman Mattford (2004) *apud* Huang, Rau **&** Salvendy, (2010)).

Muitas abordagens foram desenvolvidas para auxiliar na gestão da segurança da informação e na limitação de ocorrências de incidentes e violação de segurança. Almeida (2007) complementa essa perspectiva tecnológica de segurança da informação esclarecendo que:

> Um evento corresponde a uma alteração no estado do sistema ou dispositivo. A alteração é resultado de ações (autenticar, ler, copiar, etc.) direcionadas a objetos (conta, processo, dado, rede, etc.). Um evento pode ser parte de um conjunto de processos que objetivam ocorrências não autorizadas. Esse evento é, então, parte de um ataque. Um ataque utiliza uma ferramenta (comando, script, etc.) para explorar a vulnerabilidade de um dispositivo, que corresponde a uma falha no sistema e permite ação não autorizada. A vulnerabilidade pode ser de projeto, de implementação ou de configuração. Além disso, ela provoca um evento e gera um resultado não autorizado

> (acesso indevido, roubo de recursos, etc.). Um grupo de ataques que envolve diferentes agentes, objetivos, locais, ou horários é denominado incidente. Um incidente é um ataque associado a um objetivo, que pode ser, ganho político ou financeiro, danos ou prejuízos, dentre outros (Almeida, 2007, p.158).

A maioria dos controles desenvolvidos implica em *check lists*, análise de risco, avaliação e métodos. Entretanto, há a necessidade de se questionar essas abordagens com foco estreito, soluções tecnicamente orientadas que ignoram os aspectos sociais dos riscos e da estrutura informal de organizações (KOSKOSAS, CHARITOUDI **&** LOUTA, 2008). Apesar de toda evolução nos controles técnicos, promovida por mudanças tecnológicas constantes, as organizações devem ter em mente que sua maior vulnerabilidade é seu colaborador, por isso as empresas devem enfocar os fatores humanos, suas percepções e expectativas, em detrimento da objetividade inerente à tecnologia (COLWILL, 2010).

O fato de alguns controles técnicos como, por exemplo, os *firewalls* serem executados de maneira relativamente rápida e muitas vezes fornecerem resultados imediatos em relação aos controles formais e informais, não quer dizer que esta seja uma solução singular e independente. Os controles técnicos dependem de controles formais para determinar seu uso e funcionalidade, já os controles formais dependem de controles informais para funcionar bem. Um exemplo que esclarece essa questão é pensar sobre a senha. O controle de acesso através da senha é uma medida técnica, entretanto, se a senha estiver disponível no monitor há uma violação dos controles formais que atingem os controles técnicos.

No entanto, se há instruções formais em vigor e falta de entendimento do usuário sobre a necessidade de proteger sua senha e não expô-la em seu monitor ou em sua estação de trabalho (um controle informal), é a falta de conscientização a causa da violação. Ressalta-se que, quando um controle formal é posto em cheque, o erro se propaga tornando o controle técnico ineficaz. Assim, a eficácia da aplicação de controles técnicos pode ser ampliada e melhorada através da robusta aplicação de controles formais. Paralelamente, os controles informais facilitam a aplicação dos controles formais, ampliando e melhorando a sua eficácia (SVEEN, TORRES **&** SARIEGI 2009).

Independentemente da força de controles técnicos, se os fatores humanos e organizacionais afetam sua implementação e utilização, o efeito sobre a segurança pode ser grave (BISHOP, 2002 *apud* KRAEMER, CARAYON **&** CLEM, 2009). A este

respeito, computador vulnerável e proteção de segurança da informação (por exemplo, senhas fracas ou má usabilidade) e intenções maliciosas podem definir o cenário de vulnerabilidades para a segurança do computador e da informação (KRAEMER, CARAYON **&** CLEM, 2009).

Os fatores humanos e organizacionais influenciam os controles técnicos em vigor e as práticas atuais e a interdependência entre os três tipos de controles pode ser notada, tanto em sua implementação quanto em sua utilização (KRAEMER, CARAYON **&** CLEM, 2009). Essa interferência de elementos distintos na tecnologia é mais um indicativo que ratifica a impossibilidade de tratar a tecnologia isoladamente e basear suas práticas de segurança da informação quase inteiramente em soluções técnicas (SVEEN, TORRES **&** SARIEGI, 2009).

A metáfora da casa pode ser usada para ilustrar essa dependência. Os controles informais proporcionam uma forte fundação, os controles formais são paredes resistentes que são construídas sobre a fundação e que dão sustentação ao telhado, que constitui o controle técnico. A fundação, as paredes e o telhado da casa se apoiam mutuamente para fornecer abrigo contra chuva, vento e frio, ou seja, no caso da gestão da segurança da informação, os controles se apoiam reciprocamente contra ataques e /ou incidentes. (SVEEN, TORRES **&** SARIEGI 2009)

Ao tentar encontrar pistas que venham a contribuir para uma solução, mesmo que parcial, para a pergunta desta seção, pondera-se através de uma analogia entre a pergunta desse capítulo e a proposta dos autores KOSKOSAS, CHARITOUDI **&** LOUTA (2008), que uma das possibilidades de ocorrência de falhas de segurança deve-se ao fato dos grupos e gerentes que seguem os procedimentos de segurança não serem convocados e responsabilizados pela definição de metas de segurança relevantes para a gestão da confidencialidade, integridade e autenticidade de dados em sistemas de informação da organização.

Outro ponto é o fato da cultura ser um forte indicador no processo de definição de metas de eficiência e fixação de marcos de segurança. Os autores indicam que um forte alinhamento de cultura e disposição das metas tem um efeito sobre a maneira pela qual as metas de segurança estão definidas (KOSKOSAS, CHARITOUDI **&** LOUTA, 2008).

Analogamente, KOSKOSAS, CHARITOUDI **&** LOUTA (2008), ressaltam a importância dos cursos de educação e formação de membros para adequada percepção

dos riscos em matéria de segurança e pontuam que esta percepção reflete no sucesso global dos projetos de segurança de informação em sistemas. Compartilhamento de informações e experiências sobre o tema segurança também foram ressaltados e os autores concluem enfatizando que cultura e estabelecimento de metas são inter-relacionados e podem ter um efeito sobre sistemas na gestão de segurança da informação.

Já para Kraemer, Carayon **&** Clem (2009) os fatores humanos e organizacionais têm um papel significativo no desenvolvimento de vulnerabilidades no âmbito da segurança da informação e destacam essa complexa relação dividindo os fatores em nove áreas: influências externas, erro humano, gestão, organização, desempenho e gestão dos recursos, questões de política, tecnologia e treinamento. Os autores complementam sua análise dizendo que os profissionais de segurança e gestão devem estar cientes da multiplicidade dos papéis dos fatores humanos e organizacionais e das vulnerabilidades no âmbito da segurança da informação, sendo que estas vulnerabilidades não são originárias apenas de uma base tecnológica com problema ou erro de programação. Desta forma, o desenho e a gestão de sistemas no âmbito da segurança da informação precisam de uma abordagem integradora e multicamadas para melhorar o desempenho geral da gestão de segurança da informação.

Outro aspecto é entender que falhas de segurança podem ser geradas a partir de ameaças internas. Segundo Colwill (2010) a maioria dos ataques físicos e eletrônicos podem ser assistidos ou conduzidos por um "*insider*", mas alguns ataques só podem ser cometidos pelos *insiders*, como a liberação não autorizada de informações ou a sabotagem de bens que só os funcionários podem acessar. Às vezes, mesmo aparentemente inofensivos, os colaboradores podem ter acesso para executar uma atividade privilegiada e com isso causar danos acidentais graves, por exemplo, inadequado acesso à internet que além de desperdiçar o tempo e os recursos da organização, pode também colocar a rede da organização e sistemas em risco de infecções de vírus e *malware*; levar a possíveis ações em uma ampla gama de áreas, por exemplo, a ação criminosa, violação de direitos autorais e reclamações de assédio sexual, racismo ou assédio moral e difamação; levar a um impacto significativo na reputação da organização e receitas futuras. Todas essas possibilidades foram abordadas pela revista *The Economist Intelligence Unit* (EIU, 2009), que relata aumento no

número de organizações prejudicadas por perda de informação sensível e sigilosa que vieram parar em *blogs* e *sites* de redes sociais.

Por essas e outras questões, observa-se que a segurança não está acompanhando as mudanças tecnológico-sociais no local de trabalho. A ameaça dos empregados por negligência ou ignorância frente a questões de segurança é susceptível de ser exacerbada quando as pessoas fundem trabalho e vida pessoal. O Centro Nacional de Computação afirma que os indivíduos têm dificuldade em ter uma verdadeira fronteira entre o trabalho e a vida pessoal e que eles gastam tempo compartilhando informações pessoais e profissionais em *sites* e redes sociais com a "inocência e confiança". Esta constatação deixa o colaborador e, consequentemente, a organização abertos a uma gama de downloads de pornografia e música e a uma variedade de ataques de *malware*. Existe uma crescente pressão sobre as empresas para dar liberdade maior aos colaboradores, entretanto essa medida precisa do aparato tecnológico apoiado a regras claras e regulamentos definidos para prevenir uma descida ao caos (COLWILL, 2010).

Um ponto interessante constatado na pesquisa de Colwill (2010) são as falhas de segurança geradas pelo uso de dispositivos de dados portáteis por parte dos "*insiders*" da organização, facilitando assim o comprometimento da informação da organização. Fazendo uma leitura da pesquisa de Kavanagh (2006), Colwill (2010) observou que 89% dos trabalhadores usavam dispositivos portáteis de cunho pessoal na rede das empresas nas quais trabalhavam pelo menos uma vez por semana e que mais da metade das empresas pesquisadas do Reino Unido não tinham controles para gerenciar o uso de dispositivos de mídia removível. Paralelamente, pessoas que trabalhavam em uma empresa financeira em Londres carregavam livremente CDs nos sistemas da empresa apesar das orientações e advertências. O fato é que a política de segurança, os controles, as orientações e os treinamentos não recebem prioridade de ação, alteração e atualização por parte das empresas. A maioria dos executivos da EIU (2009) alegaram que suas empresas elaboraram políticas de tecnologia da informação para regem o uso de dispositivos, aplicações e *websites* por parte dos funcionários, entretanto, somente alguns começaram a incutir estas orientações nas mentes dos colaboradores. Destes apenas 21% das empresas pesquisadas fornecem treinamento sobre a utilização de dispositivos de comunicações pessoais e apenas 17% fazem isso para aplicações de

redes sociais. Ainda mais preocupante é que apenas 20% das empresas pesquisadas têm planos para aumentar a consciência no futuro (COLWILL, 2010).

O desenvolvimento de modelos de segurança e soluções não é suficiente para proteger os recursos informacionais. As medidas de segurança técnica têm de ser desenvolvidas e implementadas, concomitantemente com medidas de caráter legal, para prevenir e evitar o crime que utiliza computadores e redes de telecomunicações como um alvo (novas tecnologias - novos crimes) ou usa as tecnologias da informação e da comunicação como um meio para realizar um crime (crimes antigos com uma nova tecnologia) (GHERNAOUTI-HELIE, 2009).

Através da gestão da segurança, vê-se que as atuais abordagens gerenciais não atendem requisitos de transparência e controle de segurança. Toda a questão da segurança da informação é sobre a organização, proteção e defesa dos valores, tendo em conta a vulnerabilidade intrínseca das tecnologias da informação e da ameaça penal nas estratégias das instituições. Hoje, na maioria das tecnologias da informação e da comunicação, usuários finais simplesmente não compreendem as questões de segurança e não tem a habilidade, conhecimento e/ou as ferramentas corretas para proteger seus ativos. Eles não têm os meios objetivos para construir a confiança em infraestruturas e serviços de tecnologia da informação e da comunicação. Estes usuários contam com produtos, mecanismos e soluções impostas por motivos comerciais, ficando o entendimento e a consciência sobre as formas de assegurar-se na obscuridade. Acredita-se que, através do desenvolvimento de uma perspectiva interdisciplinar da segurança da informação, promover-se-á uma melhor abordagem, mais integrada e abrangente e que venha trazer valor no domínio dos riscos informativos (GHERNAOUTI-HELIE, 2009).

A interação entre pessoas e tecnologia chama a atenção para fatos atuais que podem ser remontados para se obter uma vantagem competitiva para a segurança da informação. Ghernaouti-Helie (2009) em sua pesquisa relata que fogo, terremoto, tempestade, fraude ou crime fornecem relatórios de informações para autoridades civis. Por exemplo, a Amber Alert tem mais de 7 milhões de usuários que ajudam com informações sobre o rapto de crianças, já a *PatientsLikeMe* tem atraído atenções no que concerne a questões de saúde como o bem-estar, a cessação do tabagismo, a redução da obesidade etc. Estes exemplos são tentativas primárias de insinuar o vasto potencial para a tecnologia mediada pela participação social, e ratificar a necessidade de desenvolver uma pesquisa substancial que trabalhe a persuasão e a ampliação, de modo

que aumente a motivação, o controle a ataques maliciosos, limite os boatos equivocados e proteja a privacidade.

Por isso, a tecnologia persuasiva chama a atenção como um meio para criar interação entre computação e sistemas de modo a alterar atitudes e comportamentos das pessoas (NARITA **&** KITAMURA, 2010) como uma das formas de se reduzir falhas de segurança.

Fica a necessidade das tecnologias serem menos vulneráveis para diminuir o número de potenciais ameaças que podem ser desenvolvidas (GHERNAOUTI-HELIE, 2009) e, paralelamente, vale ressaltar a necessidade de uma conscientização prévia sobre questões da segurança da informação, uma vez que se constatou que a referida "consciência" sobre questão de segurança da informação, na maioria dos casos, não ocorreu com a introdução de novas tecnologias, mas sim através de incidentes vivenciados após a sua introdução (SVEEN, TORRES **&** SARIEGI, 2009). Conforme dito por KRAEMER, CARAYON **&** CLEM (2009) a tecnologia e segurança da informação têm se concentrado em soluções tecnológicas para evitar vulnerabilidades e ataques, entretanto essas áreas precisam se relacionar, através de uma abordagem sócio-técnica, com aspectos humanos e organizacionais, uma vez que estes corroborarão diretamente na eficácia de outros sistemas críticos, tais como segurança e redução de incidentes.

A contribuição dessa seção para a construção do instrumento de coleta de dados se concentra em entender como falhas de segurança são geradas a partir da interação entre a tecnologia e os seres humanos.

Foram delineadas várias variáveis que podem servirão de base para construção do modelo medidor de segurança informacional corporativa.

As informações levantadas que se transformaram em questões no instrumento de coleta de dados são:

- A segurança da informação na instituição na qual trabalho é responsabilidade apenas do setor de tecnologia da informação.
- O desenvolvimento da segurança da informação na instituição na qual trabalho inclui proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo, sejam elas internas e/ou externas à organização.

- Eu sou orientado ou obrigado a fazer back-ups diários das informações por mim processadas em um servidor disponibilizado pela instituição.
- Eu observo, ao utilizar o meu e-mail corporativo, que ocorre a supressão de mensagens que possuem anexos não solicitados.
- A instituição permite que eu acesse a rede corporativa, grave dados em pen-drives, CD´s, DVD´s e/ou imprima informações para uso tanto no ambiente institucional quanto em casa.
- No ambiente corporativo eu tenho acesso irrestrito a todos os sites que precisar ou quiser consultar.
- Altero mensalmente minhas senhas de acesso aos recursos corporativos (por exemplo: redes, computadores, mídias removíveis etc.).
- Normalmente, acesso os sistemas de informação corporativos de minha casa (acesso remoto) para resolver algum problema ou atender a alguma demanda.
- Existe um check list de segurança da informação que devo seguir no meu dia-a-dia.

4- Metodologia de Pesquisa

Em sentido genérico, o método de pesquisa significa a escolha de procedimentos sistemáticos para a descrição e explicação de fenômenos. Esses procedimentos se aproximam dos seguidos pelo método científico, que consiste em delimitar um problema, realizar observações e interpretá-las com base nas relações encontradas, fundamentando-se, se possível, nas teorias existentes (RICHARDSON, 2007).

O presente estudo seguirá as diretrizes de uma pesquisa *survey*, uma vez que serão observadas várias características dos elementos de uma determinada população ou amostra, utilizando-se questionários ou entrevistas como instrumentos de pesquisa. A observação será feita naturalmente e sem interferência do pesquisador (BABBIE, 1999; RICHARDSON, 2007). Pretende-se, através deste estudo, registrar, analisar e correlacionar fatos e/ou fenômenos com a maior precisão possível e, por esse motivo, foi escolhido o método quantitativo com a intenção de garantir a precisão dos resultados, evitar distorções de análise e interpretação, possibilitando uma margem de segurança quanto às inferências (BABBIE, 1999; RICHARDSON, 2007). Ressalta-se que o método quantitativo será usado majoritariamente, nesse sentido pode-se dizer que haverá a utilização do método misto, ou seja, quali-quantitativo.

A pesquisa debate a temática segurança da informação, ocorrência que por sua própria natureza remete ao fato de ser algo que as pessoas não gostam de comentar e fornecer informações à respeito. Dessa forma a pesquisa segue diretrizes do menor envolvimento possível do pesquisador com o respondente, dando a ele (respondente) toda liberdade para se expressar em anonimato.

A pesquisa de ordem quantitativa tem como uma de suas características relevantes, conforme Gunther (2006), a negação ou tentativa de controle do envolvimento emocional do pesquisador com seu tema de investigação.

Dada essa introdução metodológica, as demais seções da metodologia de pesquisa seguirão o seguinte detalhamento: Fins da pesquisa, meios de investigação e raciocínio lógico; Tipos e Procedimentos da pesquisa; Sujeitos, Local de Pesquisa e Plano de Recrutamento;

4.1 Fins da Pesquisa, Meios de Investigação e Raciocínio Lógico da pesquisa

Como essa seção é dedicada a dar mais detalhes sobre as abordagens metodológicas utilizadas nesse estudo sobre segurança da informação na perspectiva de pessoas, processos e tecnologias, acredita-se que todo esse detalhamento metodológico propiciará o arcabouço necessário para desenvolvimento da pesquisa de campo.

Dessa forma, quanto aos fins, a abordagem dessa pesquisa se caracteriza pela exploração. Nesse método, os pesquisadores desenvolvem conceitos de forma mais clara, estabelecem prioridades, desenvolvem definições operacionais e melhoram o planejamento final da pesquisa. Em termos mais técnicos, uma análise exploratória de dados consiste na busca de um padrão ou modelo que possa nos orientar em análises posteriores (BABBIE, 1999; RICHARDSON, 2007).

Destarte, os meios de investigação da pesquisa são a pesquisa de campo e o estudo de caso. Segundo Brasileiro (2012, p.34), a pesquisa de campo é uma investigação realizada *in loco*, através da aplicação de questionários, entrevistas, testes, observações, na tentativa de explicar um fenômeno ocorrido. O objetivo da pesquisa de campo é a coleta de dados.

Já com relação ao estudo de caso, Gunther (2009, p.205) diz que ele é delimitado como a coleta e análise de dados sobre um exemplo individual para definir um fenômeno mais amplo, podem-se coletar e analisar tanto dados quantitativos quanto qualitativos.

Brasileiro (2012, p.34) destaca que o estudo de caso é um estudo profundo e detalhado de um determinado caso que exemplifique o assunto abordado, podendo ou não ser realizado no campo. No caso dessa pesquisa o estudo será realizado no campo.

Assim, para que se consiga entender a interferência do elemento humano na segurança da informação, a pesquisa será aplicada em uma organização privada na área de saúde, cujo nome não será divulgado a pedido da instituição.

No que concerne ao raciocínio lógico empregado na pesquisa, ela pode ser caracterizada como dedutiva, haja vista que procura explicações e generalizações probabilísticas. Segundo Moraes (1999) na pesquisa dedutiva a teoria precede à análise e serve de fundamento para ela. No caso da pesquisa sobre *segurança da informação:*

pessoas, processos e tecnologias seguiu-se exatamente a diretriz de Moraes (1999) desenvolvendo toda a parte de revisão de literatura, para que dela pudessem ser extraídos os elementos para composição da pesquisa de campo.

Voltando ao caráter dedutivo da pesquisa, complementa-se que as teorias aparecem no contexto das explicações e explicar um acontecimento, teoricamente, equivale a deduzir um enunciado que descreve esses acontecimentos, partindo-se de algumas premissas (CASSIANI, CALIRI, PELÁ, 1996, p.81).

> A abordagem dedutiva-verificatória-enumerativa-objetiva parte de teorias e hipóteses propondo uma testagem ou verificação das mesmas dentro dos cânones da pesquisa tradicional. As hipóteses ajudam a direcionar o processo, definindo juntamente com a teoria a natureza dos dados e sua organização. Por esta razão, nesta abordagem as categorias são fornecidas ou estabelecidas a priori, seja a partir da teoria, seja dos objetivos ou das questões de pesquisa. De qualquer modo nesta abordagem as categorias necessitam ser justificadas a partir de um sólido fundamento teórico. A adoção desta abordagem, em geral, implica a utilização da quantificação como tratamento preferencial dos dados, culminando em testes de hipóteses que possam levar a inferências justificadas dentro de padrões estatísticos da pesquisa quantitativa. Também nesta abordagem a objetividade é altamente considerada, mesmo reconhecendo que isto possa resultar em perda de informação preciosa que porventura as mensagens carreguem, mas que não se enquadrem nas categorias definidas à priori (MORAES, 1999).

Na sequência há referência sobre os tipos e procedimentos da pesquisa. Nota-se que os autores tomaram a iniciativa de topificar os elementos metodológicos, presumindo que dessa forma facilitariam a compreensão do leitor.

4.2 Tipos e Procedimentos da pesquisa – Aplicação Prática

Ao aplicar os tipos e procedimentos de pesquisa ao estudo prático, destaca-se que não se pode perder de vista o objetivo da pesquisa. Assim, na instituição pesquisada, busca-se identificar os perfis dos usuários e, através de uma análise cruzada, quantificar esses perfis e possíveis ações comportamentais que possuam inter-relação com falhas de segurança da informação. Examinados esses elementos, espera-se identificar circunstâncias nas quais as falhas de segurança ocorrem, a natureza dos incidentes de segurança informacional e sua razão para explorar como e o porquê das ocorrências e saber lidar com elas.

Destarte, para atingir tais objetivos, pensou-se em dividir a pesquisa nas fases de definição sujeitos, local da pesquisa, tipo de amostra e plano de recrutamento, levantamento e, por fim, análise e cruzamento de informações.

4.2.1 Seleção do Caso: Sujeitos, Local de pesquisa, Plano de Recrutamento

Para que se consiga entender a interferência do elemento humano na segurança da informação, a pesquisa será aplicada em uma organização privada na área de saúde do estado de Minas Gerais, localizada na cidade de Belo Horizonte, cujo nome não será divulgado a pedido da instituição. A população-alvo desta pesquisa são os funcionários do setor de tecnologia da informação de uma instituição privada na área de saúde.

Com relação à análise crítica de risco-benefício, pode-se dizer que a pesquisa apresenta risco mínimo ligado à possibilidade de sentimento de constrangimento ou ameaça por parte do sujeito da pesquisa. Em compensação, considera-se que o benefício é institucional, uma vez que os resultados possibilitarão ações estratégicas de melhoria da segurança informacional.

4.2.2 Diagnóstico: Coleta de Dados Documentais e Dados do Questionário

Nessa etapa, a proposta é identificar e levantar todas as práticas de segurança da informação em vigor na empresa. Para executar essa ação, tem-se em mente desenvolver uma análise documental de tudo que se refere à segurança da informação e que circula na organização para que se consiga identificar e levantar as práticas de segurança atualmente em vigor na instituição analisada.

Para que se consiga entender o posicionamento atual da organização com relação à segurança da informação corporativa, é imprescindível que se faça a análise das políticas, normas, procedimentos e documentos em vigor na instituição.

Doravante, para concluir tal ação, traçou-se como estratégia, primeiramente, levantar se os documentos com informações sobre segurança da informação da instituição são físicos ou virtuais, ou se são físicos e virtuais. A segunda ação seria solicitar cópia de tal documentação.

Visando elucidar a questão entrou-se em contato com o responsável pela área de segurança da informação da instituição pesquisada, que informou que os documentos são disponibilizados em formato físico e virtual e disponibilizou cópia dos documentos em formato eletrônico.

Como se trata de uma organização privada foi solicitado ao gerente da área cópia das políticas em vigor na organização. As políticas possuem formato documental e digital, sendo o conteúdo de igual teor em ambos os casos. Serão encaminhadas ao pesquisador as políticas em formato digital para que se proceda com a análise.

De posse do material para efetivar as análises, primeiramente definiram-se quais seriam os itens verificadores de análise. Nesse sentido, optou-se por utilizar os mesmos elementos eleitos para a composição do questionário. Todos esses elementos foram retirados da revisão de literatura. Essa parametrização permite seguir a mesma linha de análise, independente do conteúdo ser advindo de uma fonte secundária ou de uma fonte primária.

A etapa final foi a confecção de um instrumento de análise de que disponibilizasse todos os itens verificadores (elementos de análise), as políticas, normas e procedimentos da instituição e um espaço para que se procedesse o cruzamento das informações e descrição das percepções e análises do pesquisador frente aos fatos.

Destaca-se que essa fase trará contribuições substanciais à pesquisa, uma vez que é através do presente estudo que será possível identificar o estado em que se encontra a instituição arguida no que concerne às práticas de segurança da informação. Além disso, essa fase propiciará o conhecimento sobre o atual posicionamento da organização frente às questões de segurança para, a partir de então, avaliar os cenários, integrando as práticas de segurança ocorridas nas instituições, os perfis dos usuários e descobrir possíveis gargalos.

Finalizada essa etapa, pretende-se, na sequência, desenvolver questionário estruturado com base em um conjunto de variáveis que compõe cada arena – pessoas, processos e tecnologias previamente levantadas na literatura. Esse instrumento quantitativo é inédito e será aplicado junto aos colaboradores constantes na amostra da

instituição pesquisada, através de *link* encaminhado ao *e-mail* deles. As respostas ao questionário, sem identificação do respondente, serão armazenadas no *site* http://www.kwiksurveys.com/, ao qual somente o pesquisador terá acesso. Ressalva-se que os instrumentos terão como característica o anonimato, de modo que não se corra o risco de obter uma análise individual do colaborador que venha a prejudicá-lo, no sentido de sanções e/ou mesmo demissões. Não se pretende avaliar o colaborador e sim a equipe. Outra característica importante é a não interferência do pesquisador na condução das perguntas junto aos respondentes.

4.2.3 A Construção do Instrumento de Coleta de dados

O instrumento quantitativo de coleta de dados denominado questionário, conforme Barbetta (2007), deve ser cauteloso, uma vez que deve ser completo no sentido de abranger as características necessárias para atingir aos objetivos da pesquisa. Ao mesmo tempo, não deve conter perguntas que fujam desses objetivos, pois quanto maior o questionário menor tende a ser a confiabilidade das respostas.

O questionário foi estruturado em duas partes. A primeira com o objetivo de obter o perfil do entrevistado, com relação ao sexo e escolaridade. A segunda parte, composta por 49 afirmativas, seguiu uma estrutura matricial com uma escala tipo Likert. A escala de Likert é uma escala de mensuração itemizada, também denominada de "escala multi-itens". Exige que os entrevistadores indiquem um grau de concordância ou discordância com cada uma de uma série de afirmações. Os dados geralmente são tratados como intervalares, assim, a escala Likert possui as características de descrição, ordem e distância (MALHOTRA, 2012). É importante salientar que, neste trabalho, optou-se por trabalhar com 4 itens, sem ponto neutro, sendo os extremos: "(1) Discordo totalmente" e "(4) Concordo totalmente". A escala utilizada, segundo categorização de Malhotra (2012) pode ser classificada como balanceada, pois apresenta número igual de categorias favoráveis e desfavoráveis e forçada, pois os entrevistados foram forçados a emitir uma opinião, não havendo a posição neutra, ou seja, para cada afirmativa, o respondente tinha necessariamente que discordar ou concordar.

A análise pode ser feita item por item ou calculado um escore total (somatório) para cada entrevistado, somando-se os itens. Nesse estudo serão utilizados os dois métodos.

Traz-se à ciência do leitor que o questionário apresenta seis afirmações negativas. É importante destacar que a afirmação negativa não prejudica a análise dos dados do questionário, embora ao inverter o escore deste item, supõe-se que o entrevistado concordaria com o inverso da afirmativa. A estruturação em afirmações negativas contempla, conforme Malhotra (2012), a necessidade de utilizar um processo coerente de atribuição de escores. Dessa forma, categorias atribuídas pelos respondentes como respostas negativas seriam escalonadas em ordem inversa a da escala.

> Para uma afirmação negativa uma concordância traduz uma resposta desfavorável, enquanto para uma afirmação positiva a concordância representa uma resposta favorável. Consequentemente, uma resposta concordo totalmente a uma afirmação favorável, e, uma resposta discordo totalmente a uma afirmação desfavorável receberiam ambas escore 4 (MALHOTRA, 2012, P.222).

Para o uso do somatório e para a análise de cada item, as categorias atribuídas pelos respondentes às afirmações negativas, devem ser escalonadas em ordem inversa à da escala. Para uma afirmação negativa, uma concordância traduz uma resposta desfavorável.

De posse do questionário pronto e realizadas as análises, o mesmo foi publicado no site kiwiksurveys.com e procedeu-se com o pré-teste.

4.2.4 - Metodologia para Análise de dados

Esta fase da metodologia será feita organizando, resumindo e apresentando os dados de modo que se consiga interpretá-los. Desta forma, considera-se importante tratar os dados e apresentá-los em tabelas e gráficos (BARBETTA, 2007).

De posse dos dados levantados nas fases anteriores, iniciar-se-á a fase de análise dos dados, conforme descrito anteriormente. O primeiro elemento que será validado através dos dados é se as práticas de segurança da informação desenvolvidas na

instituição atendem aos requisitos de uma abordagem tecnicamente orientada ou de uma perspectiva sociotécnica, com base na revisão bibliográfica.

O problema da pesquisa direciona para a necessidade de encontrarmos na pesquisa de campo um arcabouço para a ocorrência de incidentes de segurança informacional que prejudiquem a segurança da informação da empresa. Nesse sentido, tem-se que um dos caminhos para se chegar a essa conclusão analisando os questionários e através deles inter-relacionar as falhas de segurança informacional ao enfoque dado pela empresa, no que concerne à segurança da informação. Isso quer dizer que as falhas na segurança informacional da empresa podem ter como decorrência o posicionamento da instituição através de uma abordagem contingencial, sistêmica e holística ou através de uma abordagem egocêntrica, prescritiva e exclusivamente tecnológica para a segurança da informação. Assim, encontrar respostas à questão de se a organização trata a segurança da informação através de uma perspectiva tecnicamente orientada ou sociotécnica, será fundamental para entender o foco da instituição e sua conexão, ou não, com falhas de segurança informacional. Dessa forma é possível saber como lidar com tais falhas e propor mudanças.

Para a análise, cada afirmação recebeu um escore numérico, variando de 1 a 4. A análise foi feita item por item (análise de perfil) e o escore total (somatório) para cada entrevistado. A análise de somatório é a mais comum e por isso a escala de Likert é também conhecida como a escala somatória. Para utilizar o somatório é importante utilizar um processo coerente de atribuição de escores, de modo que um escore alto reflita sistematicamente uma resposta favorável. Para isso, as categorias atribuídas pelos respondentes a afirmações negativas foram escalonadas em ordem inversa à da escala.

Com os dados tabulados o pesquisador procederá com a avaliação destes e será proposta a descrição dos resultados obtidos com base nas respostas.

Os cenários serão formulados a partir dessas análises. A avaliação de cenários propiciará entendimento acerca do atual posicionamento da segurança informacional da instituição.

A possibilidade de avaliar cenários é importante principalmente no sentido de se verificar se o mecanismo de coleta de dados atingirá o objetivo proposto, no sentido de constatar se os elementos das arenas pessoas, processos e tecnologias estão sendo abordados de forma equilibrada na gestão de segurança da informação corporativa e em qual direção os esforços de mudança devem ser direcionados.

Através do cruzamento das informações das análises feitas haverá possibilidade de verificar se os mecanismos desenvolvidos na pesquisa são suficientes para que se faça uma avaliação de cenário organizacional, no que concerne à segurança da informação, e se proponha ações de mudança.

Destarte, além dos ganhos da instituição com a pesquisa, é o ganho da pesquisa em si, sendo essa uma das grandes contribuições que a pesquisa sobre Segurança da Informação deixa para a área e para a sociedade que é a de ter um instrumento de coleta de dados sobre segurança da informação testado e ratificada a possibilidade de uso desse instrumento em outros estudos sob a ótica exploratória da pesquisa. Trata-se, conforme dito, de um modelo inédito cuja abordagem é sistêmica que tem o propósito de executar análises de cenário sob a perspectiva de segurança informacional, com o objetivo de propiciar às empresas relatórios de cenários de onde devem ser destinados os investimentos em segurança da informação. Atende-se, nessa perspectiva, o objetivo específico da pesquisa de deixar contribuições para área de Ciência da Informação que receberá um instrumento de coleta de dados para pesquisas futuras.

Paralelamente, outro aspecto passível de desenvolvimento é verificar se há possibilidade de se coligir e analisar os dados. O objetivo é determinar o curso de medidas corretivas a serem adotadas pela empresa para tratar os casos decorrentes da pesquisa.

A opção por métodos mistos de pesquisa, quantitativos e qualitativos, deve-se ao fato de que, no processo de construção de conhecimento, idealmente, o pesquisador não deveria escolher entre um método ou outro, mas utilizar as várias abordagens, qualitativas e quantitativas que se adéquam à sua questão de pesquisa. À medida que perguntas de pesquisa frequentemente são multifacetadas, comportam mais de um método e cabe ao pesquisador usar a abordagem teórico-metodológica que permita, num mínimo de tempo, chegar a um resultado que melhor contribua para a compreensão do fenômeno e para o avanço do bem-estar social (GUNTHER, 2006).

A seguir proceder-se-á com a validação do instrumento de coleta e a análise descritiva dos dados.

4.2.5 Validação do instrumento de coleta de dados

Diante da proposta da pesquisa de investigar as circunstâncias nas quais ocorrem falhas de segurança que envolvem pessoas e entender como lidar com elas, acredita-se que uma das contribuições substanciais desse estudo é deixar um instrumento de coleta de dados validado para que se consiga atingir o objetivo proposto.

Segundo Malhotra (2012) a validade de uma escala é definida como o ponto até onde as diferenças em escores observados na escala refletem as verdadeiras diferenças entre os objetos quanto à característica que está sendo medida, e não erros sistemáticos ou aleatórios. Podem ser avaliadas a validade de conteúdo, a validade de critério ou a validade de construto.

Essa validação propiciará aos interessados efetuar pesquisas que possam concluir se há uma abordagem da segurança informacional da empresa que privilegie de forma equitativa as arenas *pessoas*, *processos* e *tecnologias* ou se existe uma abordagem que seja mais favorável a alguma das arenas, gerando desequilíbrio e, consequentemente, falhas de segurança da informação.

Conforme Malhotra (2012), o processo de validação utilizará as diretrizes de uma escala multi-itens. Esse tipo de escala deve ser avaliada quanto à sua precisão e aplicabilidade, o que envolve uma avaliação da confiabilidade, validade e capacidade de generalização (dimensionalidade) da escala.

Definiu-se que, para essa pesquisa, será utilizada a validade de conteúdo ou validade nomológica. Um dos quesitos para essa validação no questionário é a determinação junto a um especialista da área, no caso da área de segurança da informação, que pode ser um dos pesquisadores ou outra pessoa, se os itens da escala abrangem adequadamente todo o domínio do construto que está sendo medido (MALHOTRA, 2012).

Essa é uma etapa imprescindível no processo de validação de um instrumento de coleta de dados, por isso Hair (2009, p.126), ressalta que no processo de validação nomológica “o pesquisador deve identificar relações teóricas a partir de pesquisa anterior ou de princípios aceitos para avaliar se a escala tem relações correspondentes”. Para a validação, foi utilizada a metodologia de validade de face ou aparente. Esta é uma avaliação subjetiva que verifica a evidência superficial da integridade da medida que o instrumento se propõe a mensurar.

Assim, a validação do instrumento foi realizada por meio de avaliação escrita e objetiva com o pesquisador autor deste trabalho e um pesquisador reconhecido da área.

As variáveis escolhidas para compor o instrumento de coleta de dados foram extraídas do levantamento bibliográfico exploratório que coleciona recortes de vários estudos sobre segurança da informação.

Na sequência, essas variáveis foram agrupadas nas arenas pessoas, processos e tecnologias. Desse agrupamento foram desenvolvidas as questões e cada uma delas foi analisada, e junto com o especialista da área foram extraídas aquelas mais relevantes para compor o instrumento de coleta de dados.

O próximo passo dessa fase foi desenvolver o item confiabilidade através do Alfa de Cronbach (MALHOTRA,2012; HAIR, 2009).

Na sequência foi desenvolvido o quesito confiabilidade e utilizou-se o alfa de C*ronbach*, que é a medida mais simples de consistência interna, para avaliação da confiabilidade. A confiabilidade de uma medida de refere à capacidade desta ser consistente, ou seja, mostra até que ponto uma escala produz resultados consistentes se as medidas forem tomadas repetidamente. Esta estatística calcula a consistência interna a partir das variâncias dos itens e dos totais do teste por sujeito, através da fórmula:

$$\alpha = \frac{k}{(k-1)} \times \left[1 - \frac{\sum_{j=1}^{k} S_j^2}{S_T^2}\right]$$

Onde k é o número de itens do instrumento, $S_j^2 = \frac{1}{n-1}\sum_{j=1}^{n}(X_{ij} - \bar{X}_j)^2$ é a variância do item $j(j = 1, \dots, k)$ e S_T^2 é a variância do total dos itens.

O alfa de *Cronbach* toma valores entre 0 e 1. Segundo Hair et al. (2009), o limite inferior para o alfa de *Cronbach* geralmente aceito é 0,70, apesar de poder diminuir para 0,60 em pesquisa exploratória. Nota-se que, nesse caso, trata-se de uma pesquisa exploratória.

Utilizando o SPSS[2], versão 19, o valor encontrado para as 49 afirmativas, do alfa de *Cronbach* foi de 0,937. Dessa forma, pode-se considerar que a escala somatória (Likert) utilizada é confiável. Com base nesse dado, pode-se dizer que o primeiro

[2] Statistical Package for the Social Sciences – Software estatístico para ciências sociais

critério de validação, que é a confiabilidade do instrumento de coleta de dados, está aceito.

Entretanto, ao analisar as considerações de Malhotra (2012), que afirma:

> Algumas escalas multi-itens incluem diversos conjuntos de itens planejados para medir diferentes aspectos de um construto multidimensional. Por exemplo, a imagem de loja é um construto miltidimensional que inclui qualidade, variedade, sortimento de mercadorias (...). Assim, uma escala planejada para avaliar a imagem de uma loja deve conter itens que meçam cada uma dessas dimensões. (...) se vários itens forem utilizados para medir cada dimensão, pode-se calcular a confiabilidade da consistência interna para cada dimensão (MALHOTRA, 212, P.230).

Concluiu-se que seria importante analisar o valor do alfa de *Cronbach* para cada agrupamento – Pessoas, Processos e Tecnologias – do questionário. Malhotra (2012) chama a atenção para o fato de que uma propriedade importante do coeficiente alfa de *Cronbach* é que seu valor tende a aumentar com o aumento do número de itens na escala. Dessa forma, o valor do alfa de *Cronbach* pode ser artificialmente inflacionado pela inclusão de vários itens redundantes na escala.

A última fase é o desenvolvimento do último item do processo de validação que é a capacidade de generalização – dimensionalidade. Segundo Malhotra (2012, p.232) a capacidade de generalização indica até que ponto um estudo baseado em uma amostra se aplica a um universo de generalizações. Vale esclarecer, segundo o mesmo autor, que essa generalização pode acontecer na proporção de uma amostra de itens para um universo de itens.

As ferramentas que serão utilizadas para proceder com a análise fatorial que mede a capacidade de generalização do questionário serão o teste KMO – Kaiser-Meyer-Olkin – e a matriz de correlação (MALHOTRA,2012; HAIR, 2009).

4.2.6 Mapeamento das fontes primárias: Análise descritiva dos dados

Nessa etapa, através da análise dos dados obtidos, haverá possibilidade de explorar como, por que e em quais circunstâncias as falhas de segurança da informação que envolvem seres humanos ocorrem.

Para tanto, se observou a necessidade da construção de um questionário cujos dados pudessem ser agrupados nas arenas – *pessoas, processos* e *tecnologias*.

Nessa linha, foi extraído, da revisão de literatura, um conjunto de elementos que pudessem trazer respostas para cada uma das arenas. Alguns elementos poderiam conduzir análises para duas ou para as três arenas simultaneamente, porém optou-se por cruzar essas informações na discussão dos resultados, com vistas a não atrapalhar a validação do instrumento de coleta de dados.

Como um dos objetivos dessa fase é analisar se as práticas de segurança da informação desenvolvidas na instituição atendiam aos requisitos de uma abordagem tecnicamente orientada ou de uma perspectiva sociotécnica para posterior leitura de cenário, a formulação das perguntas para o questionário levou em consideração o agrupamento dos elementos por arena, de modo que se consiga medições por campo – *pessoas, processos* e *tecnologias*.

Em um nível macro, pode-se dizer que serão analisadas as variáveis mais importantes que compõem os princípios definidores de cada abordagem, como: uso exclusivo de controles técnicos (tecnologia) como medidas de segurança, presença de controles formais (processos como, por exemplo, definição de políticas, medidas legais no caso de reincidência de incidentes graves), presença de controles informais (pessoas como, por exemplo, treinamentos), participação social na definição de metas de segurança, influências externas, erro humano, gestão, organização, desempenho e gestão dos recursos, ameaças internas (como por exemplo, uso de dispositivos portáteis na rede da empresa), educação, gestão da informação e do conhecimento, aprendizagem organizacional e formação. Outro fator importante é parametrizar os dados ausentes. Utilizou-se a contagem, a análise e a exposição em percentuais dos dados ausentes.

Para testar se as variáveis seguem uma distribuição normal, foi realizado o teste de Normalidade Shapiro-Wilk, pois a dimensão da amostra é inferior a 50 (MALHOTRA,2012; HAIR, 2009).. A hipótese nula testada é que os dados seguem uma distribuição normal, contra a hipótese alternativa, que os dados não seguem uma distribuição normal.

Como os dados não seguem uma distribuição normal, utilizou-se o coeficiente de correlação de *Spearman* (MALHOTRA,2012; HAIR, 2009). O coeficiente de correlação de *Spearman* (MALHOTRA,2012; HAIR, 2009), utiliza os valores das

observações em vez do valor observado, não sendo, portanto, sensível à assimetrias na distribuição para fazer correlações entre variáveis.

5- Implementação da Metodologia – Resultados

Nesse capítulo serão expressos os detalhes do percurso metodológico para se chegar aos resultados da pesquisa. Optou-se pelo desmembramento em seções para que se tenha o delineamento do passo a passo executado em cada etapa da pesquisa para se chegar aos cenários sobre segurança da informação.

5.1 – Seleção do Caso: Sujeitos, Local de Pesquisa, Tipo de Amostra e Plano de Recrutamento

Os funcionários da empresa privada na área de saúde localizada em Belo Horizonte – Minas Gerais foram convidados pelo gestor, via e-mail, a participar da pesquisa, caracterizando-se uma amostra não probabilística por conveniência. Conforme mencionado anteriormente, a pesquisa foi publicada no site http://www.kwiksurveys.com/ e encaminhada ao gestor da área de tecnologia da informação que avaliou o questionário e, na sequência, encaminhou a todos os colaboradores da área de tecnologia da informação. O universo a ser pesquisado é formado por todos os 100 colaboradores do setor de tecnologia da informação. Dos 100 funcionários convidados a participar da pesquisa, 35 (35%) responderam o instrumento de coleta de dados.

Através de pesquisas e levantamento bibliográfico a respeito de alguns conceitos sobre áreas funcionais (fim) [3] aplicados à modelagem de negócios, delimitou-se, exploratória e preliminarmente, que a informação que possui valor de ativo na instituição pesquisada é aquela focada na busca e integração de médicos (todas as especialidades), hospitais, unidades de pronto atendimento, unidades de exames gerais, serviços de diagnóstico etc., ou seja, todos os recursos humanos, físicos e virtuais necessários ao atendimento de demandas de clientes associados na área da saúde.

[3] É o ciclo de ações que envolve uma equipe multifuncional no ciclo de transformação de insumos em produtos ou serviços e de sua disponibilização no mercado.

Nota-se que todos os funcionários questionados possuem ligação com a informação que possui valor de ativo para a organização e esse foi o critério determinante para a escolha do setor no qual se deveria aplicar a pesquisa.

Acrescenta-se a esse plano de amostragem a informação de que a coleta de dados será efetuada com os elementos acessíveis na época da ação. Conforme descrito por Barbetta (2007), uma população acessível é o conjunto de elementos que queremos abranger em nosso estudo e que são passíveis de serem observados com respeito às variáveis que se pretende levantar. Assim, o universo de estudo que se pretende investigar são todos os colaboradores do departamento da instituição pesquisada acessíveis no período da pesquisa.

Não será necessária contrapartida financeira da instituição selecionada para participar da pesquisa e tampouco haverá necessidade de ceder quaisquer componentes de sua infraestrutura para realização da pesquisa.

5.2- Análise Documental e dos Dados Primários advindos do Questionário

De posse dos dados documentais que servem de base para elucidar o momento presente da instituição pesquisada e dos dados primários que foram coletados através do instrumento de coleta de dados e que nos posicionarão sobre o cenário da instituição no que concerne à segurança da informação, procedeu-se a análise e cruzamento das informações.

A análise documental das políticas de segurança da informação que estão em vigor na instituição pesquisada foi o primeiro passo. Essa é uma etapa primordial da metodologia que contribuirá para elucidação de parte do problema de pesquisa, no sentido de investigar a inter-relação do elemento humano no contexto corporativo e também contribui para o esclarecimento de parte dos objetivos específicos, abaixo citados:

1. Promover um trabalho de campo para explorar como, por que e em quais circunstâncias ocorrem falhas de segurança que envolvem pessoas e entender como lidar com elas;

2. Compreender em que medida estaria o usuário da informação corporativa, preparado e amparado para evitar falhas de segurança;
3. Investigar a inter-relação entre o usuário e a segurança da informação nas organizações, para explorar elementos indicadores de falhas de segurança, com o objetivo de compreender como as organizações podem atuar frente a problemas de insegurança informacional envolvendo recursos humanos e como podem se prevenir de tais incidentes.

Para que se proceda a análise dos dados secundários, cabe esclarecer que os resultados serão apresentados por critérios, ou seja, para cada critério de análise serão disponibilizadas a política e suas respectivas apreciações. Acredita-se que esse formato possibilitará ao leitor críticas e uma leitura comparativa.

A escolha dos critérios que serão ferramenta para análise das políticas da organização pesquisada foi extraída do questionário de coleta de dados primários. É importante que os dados da organização sejam analisados com base nos mesmos critérios do instrumento de coleta de dados, para que se possa ter parâmetros de comparação entre dados primários e secundários e uma análise uniforme dos dados coletados.

Dessa forma segue, a saber, referências das políticas da instituição pesquisada e análises dos pesquisadores.

QUADRO 1

Análise das políticas da instituição pesquisada com base no critério - Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada "transfer", visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	A política coloca que não é feito *back up* das informações dessa área de transferência e que, logo, não há responsabilidade do setor de tecnologia da informação. Essa afirmativa vincula a segurança da informação (backup) ao setor de tecnologia da informação.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Observa-se nessa política que todos os controles a autorizações para sua execução são vinculados ao setor de tecnologia da informação e não a uma comissão formada por membros de diversos setores da empresa. Esse fator remete indiretamente a uma percepção de que as ações de segurança da informação sejam de responsabilidade do setor de tecnologia da informação.

QUADRO 1

Análise das políticas da instituição pesquisada com base no critério - Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Fica claro nessa política que todas as ações para garantir a não infecção de máquinas e equipamentos da empresa são administradas pelo setor de tecnologia da informação. Inclusive em várias da políticas a expressão segurança da informação é mudada para segurança da tecnologia da informação, fato este que demonstra o viés tecnológico ao tratar das questões de segurança da informação
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	A regulamentação acerca da política de uso da internet corporativa foi delimitada pelo setor de tecnologia da informação
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	Essa política é uma responsabilidade conjunta de todos os colaboradores da organização. O descarte é feito pela pessoa que certificou o não atendimento às premissas de possuir valor histórico comprobatório ou demonstrativo de cumprimento de preceitos legais, fiscais ou contratuais; possuir valores informativos administrativo, contábil, financeiro, técnico ou operacional; conter informações sigilosas que não sejam passíveis de manutenção no arquivo morto da empresa devendo, portanto, ser descartado; ou o descarte pode ser feito também por pessoa com permissão de acesso às informações nele contidas .
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir os procedimentos relativos a esses acessos.	Essa política coloca instruções gerais que devem ser seguidas por todos os colaboradores da organização no que concerne à seguraça física do ambiente de tecnologia. Essa política traz instruções subdivididas em: áreas de acesso, áreas protegidas e áreas de segurança máxima.

QUADRO 1

Análise das políticas da instituição pesquisada com base no critério - Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Nota-se que a política determina que a autorização de acesso remoto à rede de dados e sistemas em produção seja feita pelos profissionais dos setores de Administração de Redes e Infra-Estrutura, desde que a solicitação esteja em concordância com as políticas de Qualidade em TI e Segurança da Informação
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição.	Todo o procedimento descrito na política de backups é majoritariamente de responsabilidade do setor de tecnologia da informação
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Essa política deixa claro que o setor de tecnologia da informação dará o suporte necessário ao colaborador, mas que a preservação de um ambiente seguro depende muito do comportamento e da atitude de cada funcionário.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não há referência nessa política que determine a responsabilidade exclusive do setor de tecnologia da informação

QUADRO 1

Análise das políticas da instituição pesquisada com base no critério - Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Ao analisar a delimitação nas políticas observa-se que a empresa institui um comitê que é formado pelo gestor do Núcleo de Inteligência Corporativa – NIC o gestor de Tecnologia da Informação – GTI e o responsável pelo STI, que atua como secretário desse comitê. Encontra-se também a designação para criação da área de de Segurança em Tecnologia da Informação - STI, no Departamento de TI, cujo responsável atua como secretário do Comitê de Segurança da Informação que tem por objetivo implementar essa política de segurança da informaçãp, criar mecanismos que assegurem a sua atualização, monitoramento e efetividade. Forte vínculo da segurança da informação com o departamento de tecnologia da informação.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Há uma vinculação na política de login de acesso à rede de dados e sistemas da empresa ao setor de tecnologia da informação dando autonomia a esse setor para dar e retirar acesso aos colaboradores

QUADRO 1

Análise das políticas da instituição pesquisada com base no critério - Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe alguma delimitação nas políticas que colocam a segurança da informação na instituição como sendo responsabilidade apenas do setor de tecnologia da informação?
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	No caso de solicitação de acesso à rede lógica, observa-se vinculo forte com o setor de tecnologia da informação, haja vista que o gestor de cada área da empresa deve solicitar ao setor de TI o usuário e senha para acesso à rede lógica da empresa e também delimitar junto a este a acessibilidade ao ativo informacional da empresa.

QUADRO 2

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Essa regra deixa clara a participação do usuário no processo de segurança informacional a partir do momento em que a organização determina o tipo de conteúdo que não deve ser armazenado na área denominada "transfer", o tempo de permanência admitido na área de transferência e coloca cada funcionário responsável por aquilo que armazena nesse local.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Essa política coloca o usuário como parte que vai cumprir, através de suas ações, as regulamentações constantes na política. Entende-se, entretanto, que trata-se de cumprimento passivo a empresa dita o colaborador obedece e não um cumprimento ativo no qual o colaborador participa das decisões daquilo que será necessário cumprir para garantir a segurança informacional da empresa.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Essa política de antivirus coloca o usuário como parte a partir do momento que infere a ele a responsabilidade pelo acontece com sua máquina ou equipamento. Apesar de ser uma abordagem coersitiva, ou faz ou será punido, as instruções são passadas para o usuário e tem-se a consciência de que garantir a não infecção de uma máquina ou equipamento só é possível se o usuário fizer a sua parte, como por exemplo, não baixando conteúdo da internet e nem executando arquivos recebidos via e-mail.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	O usuário é parte responsável, haja vista que o sucesso da política depende se sua observância aos critérios discriminados na política

QUADRO 2

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Essa regra deixa clara a participação do usuário no processo de segurança informacional a partir do momento em que a organização determina o tipo de conteúdo que não deve ser armazenado na área denominada "transfer", o tempo de permanência admitido na área de transferência e coloca cada funcionário responsável por aquilo que armazena nesse local.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Essa política de antivirus coloca o usuário como parte a partir do momento que infere a ele a responsabilidade pelo acontece com sua máquina ou equipamento. Apesar de ser uma abordagem coersitiva, ou faz ou será punido, as instruções são passadas para o usuário e tem-se a consciência de que garantir a não infecção de uma máquina ou equipamento só é possível se o usuário fizer a sua parte, como por exemplo, não baixando conteúdo da internet e nem executando arquivos recebidos via e-mail.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	O usuário é parte responsável, haja vista que o sucesso da política depende se sua observância aos critérios discriminados na política

QUADRO 2

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	O usuário nessa política é parte responsável, haja vista que ele pode dar a permissão para descarte de determinada documentação, haja vista que possui acesso às informações nesse documento contidas.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	O usuário é parte integrante quando segue as diretrizes propostas na política, tanto com relação a si mesmo quanto com relação à terceiros que necessitam de acesso à instituição pesquisada.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Essa política coloca o usuário como parte que vai cumprir, através de suas ações, as regulamentações constantes na política. Entende-se, entretanto, que trata-se de cumprimento passivo: a empresa dita o colaborador obedece, e não um cumprimento ativo no qual o colaborador participa das decisões daquilo que será necessário cumprir para garantir a segurança informacional da empresa.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Nota-se que uma considerável parte do processo de backup é automático. Esse fator é muito positivo principalmente no sentido de poupar o usuário de um volume muito grande atividades. É uma política que deixa claro ao usuário que os dados e informações estão sendo gravados conforme determinações acordadas na instituição e descritas na política em questão. E o usuário é responsável pela segurança a partir do momento em que existem prescrições na política que dependem de sua ação para ser efetiva.

QUADRO 2

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Essa política ressalta a grande contribuição que o usuário pode dar tendo um comportamento seguro para a proteção dos ativos informacionais da instituição.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Existe formalização na norma que o usuário, cooperados, prestadores, fornecedores e clientes, que de alguma forma têm acesso ao patrimônio de informações da empresa são responsáveis pelo cumprimento das Normas de Segurança da Informação da instituição. Assim há o vínculo mas como mecanismo executor da política e não participante.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Nessa política o usuário é parte quando possui login e senhas pessoais e intrasferíveis com vistas a acessar a rede de dados e sistemas da empresa. A criação do login ou exclusão deste é de respponsabilidade do setor de tecnologia da informação.

QUADRO 2

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação colocam o usuário como parte responsável pela segurança da informação praticada na instituição
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	O usuário é parte responsável haja vista que somente poderá ter acesso aos ativos informacionais da empresa mediante login e senha. Esse acesso depende da liberação do gestor da área na qual a pessoa vai trabalhar e de liberação do setor de tecnologia da informação.

QUADRO 3

Análise das políticas da instituição pesquisada com base no critério -Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Existe a proibição com relação ao armazenamento de arquivos que contenham informações sigilosas na área denominada "transfer". Entretanto a política não esclarece e nem coloca referência a uma outra política que esclareça quais são os critérios de classificação de informação sigilosa para que se proceda de forma a garantir a confidencialidade, disponibilidade e a integralidade das informações. Portanto pode ser que na área denominada transfer ocorra armazenamento, por tempo determinado ou não, de informação sigilosa
Utilização de mídias removíceis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Nessa política existe direcionamento claro e direto com relação ao significado dos critérios de confidencialidade, disponibilidade e integridade e como esses critérios são aplicados na prática da empresa.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Nessa política, apesar de necessária, não são explorados os critérios de confidencialidade, disponibilidade e integralidade.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Nessa política não são explorados os critérios de confidencialidade, disponibilidade e integralidade.

QUADRO 3

Análise das políticas da instituição pesquisada com base no critério -Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenha mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	A política de descarte adequado de documentos é um dos mecanismos usados pela empresa para garantir a confidencialidade das informações contidas nos documentos. Os critérios de confiencialidade, disponibilidade e integridade também são mencionadas nessa política uma vez que todo documento impresso, de procedência externa ou interna, que atender as características abaixo, deve ser arquivado em móvel adequado a essa finalidade, e, se houver condições e disponibilidade, este arquivamento deve ocorrer em meio magnético, assegurando a manutenção dos critérios supra citados.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Apesar de não haver uma menção direta, as diretrizes na política em questão objetivam auxiliar no processo de garantir a confidencialidade, disponibilidade e a integralidade dos dados e das informações no ambiente corporativo.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Indiretamente observa-se que política acaba tendo como objetivo a confidencialidade, integridade e disponibilidade dos dados e informações da empresa pesquisada. Porém, a política de acesso remoto à rede de dados e sistemas em produção não trata diretamente das formas de manter a confidencialidade, integridade e disponibilidade dos dados e informações da empresa pesquisada.

QUADRO 3

Análise das políticas da instituição pesquisada com base no critério -Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	A política não aborda diretamente as questões de confidencialidade, disponibilidade e da integralidade dos dados e informações. Entretanto observa-se que uma das finalidades dos backups seja a de garantir a confidencialidade, disponibilidade e a integralidade dos dados e informações da instituição pesquisada
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Existem alguns pontos dessa política em que os critérios de integridade, disponibilidade de confidencialidade poderiam ser explorados, entretando a organização não utilizou esse viés de abordagem.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Essa política discrimina em seu escopo esses elementos como formas de efetivação da política na prática.

QUADRO 3

Análise das políticas da instituição pesquisada com base no critério -Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem critérios de confidencialidade, disponibilidade e integridade dispostos nas políticas?
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Essa política discrimina em seu escopo esses elementos como formas de efetivação da política na prática.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Essa política discrimina em seu escopo esses elementos como formas de efetivação da política na prática.

QUADRO 4

Análise das políticas da instituição pesquisada com base no critério - Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada "transfer", visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Nessa política não há esse direcionamento.
Utilização de mídias removíceis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	A política não explora a melhoria contínua dos processos.

QUADRO 4

Análise das políticas da instituição pesquisada com base no critério - Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Nessa política seria muito importante explorar a aprendizagem organizacional desenvolvendo ações no sentido de alimentar os colaboradores daquilo que acontece dentro e fora do ambiente corporativo. Dessa forma, toda informação da investigação acerca de infecção por virus que, por exemplo, é feita pelo setor de infra-estrutura, poderia ser analisada, sintetizada e encaminhada aos colaboradores a nível informativo. Posteriormente, caso a organização deseje, um fórum de discussões poderia ser aberto e possíveis soluções poderiam ser discutidas com todos, no sentido de minimizar a ocorrência de tais problemas.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Nota-se que essa política de acesso à internet não é explorada sob o ponto de vista de contribuir com a melhoria contínua dos processos
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	A política de descarte de documentos não é explorada como fator de promoção da melhoria contínua dos processos.

QUADRO 4

Análise das políticas da instituição pesquisada com base no critério - Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	A política de acesso remoto à rede de dados e sistemas em produção não é explorada como fator de promoção da melhoria contínua dos processos.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	A política de acesso remoto à rede de dados e sistemas em produção não é explorada como fator de promoção da melhoria contínua dos processos.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	A política de acesso remoto à rede de dados e sistemas em produção não é explorada como fator de promoção da melhoria contínua dos processos.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	A política de acesso remoto à rede de dados e sistemas em produção não é explorada como fator de promoção da melhoria contínua dos processos.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 4

Análise das políticas da instituição pesquisada com base no critério - Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há um direcionamento na política organizacional de segurança da informação para que as ações de segurança da informação sejam exploradas no intuito de promover a melhoria continua dos processos institucionais.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Essa política não é explorada sob esse aspecto
Criação e alteração de login de acessos à rede de dados e sistemas da	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Essa política não é explorada sob esse aspecto
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Essa política não é explorada sob esse aspecto

QUADRO 5

Análise das políticas da instituição pesquisada com base no critério - A segurança da informação na instituição está prevista no planejamento estratégico ou na gestão estratégica da empresa?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério:A segurança da informação na instituição está prevista no planejamento estratégico ou na gestão estratégica da empresa?
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Essa política não contempla essa referência
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Nessa política não há referência a indicadores de gestão que levem em consideração a segurança da informação. Não dispõe-se da informação se a organização utiliza ou não critérios de gestão estratégica, mas pela não apresentação desses indicadores nas políticas tem-se a impressão de que a segurança da informação não faz parte da gestão estratégica ou planejamento estratégico da empresa, e, consequentemente, ainda não está totalmente integrada ao negócio da empresa.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Nessa política, observa-se a não integração das determinações aqui descritas como parte da estratégia organizacional.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Nessa política não existem informações que relacionam a política em questão e a gestão estratégica da empresa

QUADRO 5

Análise das políticas da instituição pesquisada com base no critério - A segurança da informação na instituição está prevista no planejamento estratégico ou na gestão estratégica da empresa?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério:A segurança da informação na instituição está prevista no planejamento estratégico ou na gestão estratégica da empresa?
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	Nessa política não existem informações que relacionam a política em questão e a gestão estratégica da empresa
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.
Acesso remoto à rede de dados e sistemas em	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Nessa política não existem informações que relacionam a política em questão e a gestão estratégica da empresa
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Nessa política não existem informações que relacionam a política em questão e a gestão estratégica da empresa
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Nessa política não existem informações que relacionam a política em questão e a gestão estratégica da empresa
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 5

Análise das políticas da instituição pesquisada com base no critério - A segurança da informação na instituição está prevista no planejamento estratégico ou na gestão estratégica da empresa?

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério:A segurança da informação na instituição está prevista no planejamento estratégico ou na gestão estratégica da empresa?
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Essa política fala que os recursos humanos externos à organização devem cumprir as determinações da política de segurança da informação. Entretanto, nessa política, a empresa não correlaciona proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	A proteção do harware, software, pessoas e processos se dá através de acesso autorizado e permitido às informações da empresa ou parte delas segundo os critérios de acessibilidade.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	A política em questão prevê, como forma de preservação, dos ativos informacionais da empresa, incluindo pessoas, processos e tecnologias, o acesso restrito aos ativos informacionais que são vinculados à atividade exercida e também através de login e senha pessoais e intransferíveis.

QUADRO 6

Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	O controle das visitas às dependências da organização é um tipo de proteção aos ativos tangíveis e intangíveis corporativos.
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	O controle das visitas às dependências da organização é um tipo de proteção aos ativos tangíveis e intangíveis corporativos.
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	A proteção nessa política é delimitada quando se estabelece como norma que a utilização do espaço transfer é concedida apenas aos colaboradores da instituição.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Há um direcionamento nessa política no sentido de proibir o uso de mídias removíveis e portas USB, tendo como recurso adicional o bloqueio via sistema. Entretanto existe uma ressalva para que os recursos sejam liberados caso o trabalhador precise deles para execução de suas atividades. Para isso é necessário o preenchimento de controles formais e autorização do setor de Governança de TI.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem-se na rede de computadores da instituição pesquisada.	Essa política é composta de série de recomendações no sentido de preservar a integridade das máquinas e equipamentos no ambiente corporativo. Entretanto vê-se que a organização deposita nos softwares antivirus a preservação de processos e pessoas contra ameaças e vulnerabilidades.

QUADRO 6

Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	As políticas determinam o não acesso a determinados grupos de sites previamente estipulados pela empresa. Entretanto nota-se que essa precrição não é válida para todos os colaboradores da empresa. A Diretoria, Assessorias, Superintendências e Gestões já possuem acesso, e, outras pessoas podem obter acesso a determinados grupos de sites não permitidos desde que aprovado pelo gestor.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	A proteção nos processos ocorre a partir do momento que se estabalece o descarte consciente prescrito por norma dos documentos organizacionais que contém informação sigilosa.

QUADRO 6

Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	A proteção dos ativos físicos da organização é o destaque dessa política. Nesse sentido a empresa estabelece critérios de delimitação de acesso conforme a classificação de cada área de acesso. Nota-se a existência de controles de entrada física; padrão de crachás de identificação e diretrizes no que concerne ao fato de se ter conhecimento acerca das informações que estão nas áreas de segurança máxima somente a alguns colaboradores e quando necessário; as áreas de segurança máxima devem estar fechadas e trancadas adequadamente de forma a impedir acessos não autorizados; autorização de acesso às áreas de segurança máxima; diretrizes para que materiais combustíveis e perigosos e suprimentos de quaisquer tipos não sejam armazenados em áreas de segurança máxima; uso de eletroeletrônicos, nessa área, somente mediante autorização. Sobre a segurança de pessoas nota-se importante diretriz para que os crachás de cada colaborador contenham o mínimo possível de informações sobre o colaborador.

QUADRO 6

Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	A política de acesso remoto à rede de dados e sistemas em produção é um processo que deve ser executado pelos colaboradores e parceiros da instituição pesquisada para garantir a proteção do ambiente corporativo. Não há nessa política especificações diretas com relação a hardware, software e pessoas.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Todas as instruções para realização de backups, os tipos de backups e tecnologias utilizados têm por objetivo a proteção dos ativos informacionais contra ameaças e vulnerabilidades do ambiente corporativo como um todo. Observa-se nessa política um peso maior dado às tecnologias e normas utilizadas para garantir os backups e um peso menor dado à colaboração das pessoas nesse processo de efetivação de uma política tão importante.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Nessa política fica destacada uma relação de ações que a empresa deseja que seus colaboradores adotem com o objetivo de reduzir ameaças e vulnerabilidades externas ou internas através de um comportamento seguro. O direcionador desse comportamento seguro são as normas descritas ao longo dessa política, sendo que elas envolvem questões da tecnologia como o uso de CD´s ou download de programas da internet.

QUADRO 6

Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Essa política fala que os recursos humanos externos à organização devem cumprir as determinações da política de segurança da informação. Entretanto, nessa política, a empresa não correlaciona proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	A proteção do harware, software, pessoas e processos se dá através de acesso autorizado e permitido às informações da empresa ou parte delas, segundo os critérios de acessibilidade.

QUADRO 6

Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura:
		Critério: Há instruções nas políticas que prescrevam o desenvolvimento da segurança da informação na instituição através da proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo sejam elas internas e/ou externas à organização.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	A política em questão prevê, como forma de preservação, dos ativos informacionais da empresa, incluindo pessoas, processos e tecnologias, o acesso restrito aos ativos informacionais que são vinculados à atividade exercida e também através de login e senha pessoais e intransferíveis.

QUADRO 7

Análise das políticas da instituição pesquisada com base no critério - Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada "transfer", visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Como são expostas execeções na política cujos casos permite-se usar mídias removíveis e portas USB, fica clara a necessidade de se prevenir as mídias contra incidentes maliciosos usando ferramentas de antivírus, anti-spaywares e outras disponibilizadas pela empresa. Entretanto não existe referência de caso sobre quais ações tomar frente a detecção e documentação de incidentes porventura ocorridos.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	O procedimento de instalação de software antivirus é o recursos utilizados pela organização para preservar pessoas, processos e tecnologias contra incidentes com vírus. Entretanto, quando ocorrem infecções, a empresa trata com ações corretivas e não corretivas e preventivas. A detecção do incidente e sua investigação acontece após a certeza de alguma contaminação. Apesar da política não mencionar claramente, entende-se que, como há uma investigação, uma consquência lógica seria a documentação daquilo que foi constatado até mesmo para aplicar aos responsáveis das sanções cabíveis.

QUADRO 7

Análise das políticas da instituição pesquisada com base no critério - Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Segue as mesmas orientações da política de software antivirus. A detecção do incidente e sua investigação acontece após a certeza de alguma contaminação. Apesar da política não mencionar claramente, entende-se que como há uma investigação uma consquencia lógica seria a documentação daquilo que foi constatado até mesmo para aplicar aos responsáveis das sanções cabíveis.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	A política em questão não prevê detecção, prevenção e documentação caso ocorra algum problema no processo de descarte da documentação sigilosa.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	A política em questão não prevê detecção, prevenção e documentação caso ocorra algum incidente que infrinja a segurança física do ambiente de tecnologia. Há apenas informativo na política de que os dispositivos de controle de acesso automatizado devam fornecer, quando necessário, relatórios de acessos realizados ao perímetro de segurança.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	A política de acesso remoto à rede de dados e sistemas em produção não trata da detecção, prevenção e documentação de incidentes de segurança da informação que envolva essa política.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Caso ocorra algum incidente durante as rotinas de backup estipuladas pela organização, não existe procedimento a ser seguido mencionado na política de backups. Dessa forma, como não há um procedimento definido nessa política, ela não explora a detecção, prevenção e documentação dos incidentes porventura ocorridos

QUADRO 7

Análise das políticas da instituição pesquisada com base no critério - Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Essa política previne o colaborador que quaisquer arquivos ou potenciais provas de queo colaborador foi atacado. A empresa ainda ressalta que essas provas são úteis em caso de um eventual processo judicial contra o atacante. Apesar da constatação da necessidade de documentação de possíveis ataques, nota-se que a empresa analisada ainda não trabalha coordenadamente com a detecção, prevenção e documentação dos incidentes como fonte informacional para organização e gestão, e também como mecanismo gerador de aprendizagem organizacional.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	A política de segurança da informação não trata da detecção, prevenção e documentação de incidentes de segurança da informação que envolva essa política.

QUADRO 7

Análise das políticas da instituição pesquisada com base no critério - Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há prescrição política para detectar, prevenir e documentar incidentes de segurança da informação na instituição.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	A política de acesso a redes e sistemas não trata da detecção, prevenção e documentação de incidentes de segurança da informação que envolva essa política.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	A política em questão não trata da detecção, prevenção e documentação de incidentes de segurança da informação que envolva essa política.

QUADRO 8

Análise das políticas da instituição pesquisada com base no critério - Estão claras as condutas que a instituição deseja que seus recursos humanos tenha em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Estão claras as condutas que a instituição deseja que seus recursos humanos tenham em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	As condutas estão claras, entretanto a abordagem de controle de acesso é restrita
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	As condutas estão claras, entretanto a abordagem de controle de acesso é restrita
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Nessa política são expostas ações que devem ser seguidas pelos colaboradores desde a utilização da área "transfer", o conteúdo não permitido, a permanência do conteúdo, a limpeza e o backup.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Nessa politica ficam explícitas as obrigações e cuidados de cada colaborador que usa mídias removíveis e também as sanções caso ocorram ações que contrariem a política. Nota-se que há a possibilidade de se desenvolver uma perpsectiva menos restristiva e mais colaborativa e inclusiva, como por exemplo no sentido de enconrajar a comunicação e a discussão de incidentes de segurança da informação.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	As condutas ficam restritas a uma abordagem de se executar o que se pede. No caso dessa política de software ativirus isso se restringe a não desistalar o referido software; não abrir arquivos recebidos por e-mail; não baixar conteúdo da internet; Interferir quando o software estiver realizando atualizações e/ou verificações na estação.

QUADRO 8

Análise das políticas da instituição pesquisada com base no critério - Estão claras as condutas que a instituição deseja que seus recursos humanos tenha em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Estão claras as condutas que a instituição deseja que seus recursos humanos tenham em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Assim como nas políticas anteriormente analisadas, as condutas ficam restritas a uma abordagem de se executar o que se pede. No caso dessa política de uso da internet corporativa, isso se restringe a não acessar os sites que constam no grupo de sites proibidos e usar o acesso da interne para fins de trabalho.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas	As formas de descarte estão claras e como cada pessoa deve agir para que se proceda com o descarte consciente.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	As condutas estão claras. Nota-se nessa política a presença intruções para fixar avisos nas portas, facilmente visíveis e legíveis, alertando que o acesso às áreas de segurança máxima é restrito somente às pessoas autorizadas, desestimulando qualquer tentativa de invasão. Além desse fator destaca-se que os acessos são previamente analisados e autorizados antes de serem concedidos.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Assim como nas políticas anteriormente analisadas, as condutas ficam restritas a uma abordagem de se executar o que se pede. Seguir todos os procedimentos para adquirir um acesso remoto à rede de dados ou sistema em produção

QUADRO 8

Análise das políticas da instituição pesquisada com base no critério - Estão claras as condutas que a instituição deseja que seus recursos humanos tenha em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Estão claras as condutas que a instituição deseja que seus recursos humanos tenham em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Como informado anteriormente é uma política majoriatariamente automática, sendo este um fator muito positivo para não sobrecarregar os recursos humanos com a execução da maior parte da atividade. Existe a prescrição que os colaboradores devem seguir para efetivação do backup, entretanto, trata-se de uma abordagem prescritiva.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Fica clara na política as condutas que a empresa deseja que seus colaboradores tenham para que não ocorram ataques ou incidentes de segurança que coloquem em risco os ativos da empresa. Todavia, a política praticamente não contempla os comportamentos desejados de seus colaboradores (plano B) caso um incidente ou ataque ocorra
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 8

Análise das políticas da instituição pesquisada com base no critério - Estão claras as condutas que a instituição deseja que seus recursos humanos tenha em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Estão claras as condutas que a instituição deseja que seus recursos humanos tenham em sua política de segurança da informação (Exemplo:comunicação de incidentes de segurança).
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Há uma referência no sentido de determinar a responsabilidade dos recusos humanos caso algo ocorra ao patrimônio da empresa, todavia, essas referências prevêem apenas o cumprimento das políticas e não como tratar, por exemplo, eventualidades.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Há referência que abrange os recursos humanos apenas no sentido deles efetuarem acesso às redes e aos sistemas através de login pessoal e intransferível. Entretanto essas referências prevêem apenas o cumprimento das políticas e não tratam, por exemplo, eventualidades.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	A política prevê todo o detalhamento de ações que os setores envolvidos na concessão e bloqueio de acessos deve executar. Entretanto no que concerne ao usuário final observa-se pouca exploração das condutas que o usuário deve ter.

QUADRO 9

Análise das políticas da instituição pesquisada com base no critério - Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Não se aplica
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Interessante que essa política deveria contemplar a necessidade, a periodicidade e os critérios normativos para auditar as mídias removíveis, portas USB e os computadores dos funcionários que tem ou não acesso a tal "benefício". Entretanto, não há menção na política em questão sobre o assunto. Apenas um parágrafo no qual coloca-se que a configuração de acesso como "administrador" compete apenas a profissionais específicos do setor de tecnologia da companhia e que nenhum outro funcionário está autorizado a trabalhar com tal
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Interessante que essa política deveria contemplar a necessidade, a periodicidade e os critérios normativos para auditar as máquinas e equipamentos com relação à instalação de softwares antivirus, verificação de segurança e atualização do software antivirus. Entretanto, apesar desses processos serem efetuados remotamente e em alguns casos automaticamente, não há menção na política em questão sobre auditorias.

QUADRO 9

Análise das políticas da instituição pesquisada com base no critério - Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Nessa política explicita-se que ocorrerão auditorias para monitorar acessos a conteúdos da internet, principalmente aqueles não voltados para assuntos de trabalho. Todos os acessos à Internet corporativa da empresa devem ser controlados e monitorados pelos administradores de Rede e Servidores da área de Infra-Estrutura, sendo bloqueados sites considerados pela empresa, como indevidos.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas	Haveria necessidade de se proceder com auditorias periódicas no sentido de averiguar se as instruções para descarte consciente dos documentos, principalmente os sigilosos, estão ocorrendo adequadamente. Entretando essa política não prevê a ocorrência de auditorias.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	A política em questão não menciona o uso de auditorias para verificar se as políticas estabelecidas estão sendo cumpridas.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Essa política destaca diretamente a questão das auditorias. São estabelecidos critérios diretos para o acesso, a necessidade de software de apoio de auditoria e a periodicidade dos logs de acesso para monitoramento da auditoria. A política também destaca a todos os colaboradores e parceiros que a auditoria é uma prática, que será efetivado o rastreamento dos dados para auditoria e que haverá punição em caso de violação.

QUADRO 9

Análise das políticas da instituição pesquisada com base no critério - Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Não há uma referência clara na política com relação às auditorias. A política também não determina outras formas de controle para checar se os procedimentos da política de backups estão sendo feitos, especialmente aqueles que não são automáticos.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Não há referência sobre auditorias nessa política.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Não há referência sobre auditorias nessa política.

QUADRO 9

Análise das políticas da instituição pesquisada com base no critério - Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Há referência nas políticas sobre a necessidade, periodicidade e critérios para normatizar a ocorrência de auditorias sobre segurança da informação.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Não há uma referência com relação às auditorias para acesso às redes e aos sistemas, entretanto, existe menção sobre a periodicidade de validade das senhas que são emitidas pelo setor de tecnologia da informação e que devem ser trocadas pelo ususário conforme o prazo estabelecido pela instituição.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Há referência sobre a necessidade e importância da execução de auditorias no sentido de atestar se os acessos aos ativos informacionais estão delimitados conforme controles formais.

QUADRO 10

Análise das políticas da instituição pesquisada com base no critério - As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	Esta política prevê um comportamento que a empresa deseja que seu colaborador tenha no caso de acesso de terceiros às dependências da empresa e também no caso de saída de recursos físicos e materiais da organização. Ressalta-se a necessidade de preenchimento de formulários, a existência da controles de acesso às instalações da empresa (formulários e crachás), regras para acesso em horários especiais, feriados e finais de semana.
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Esta política prevê um comportamento que a empresa deseja que seu colaborador tenha no caso de recebimento de visitas à empresa. Observa-se necessidade com relação ao preenchimento de formulários e de aprovações junto a uma equipe previamente estabelecida
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Esta política prevê um comportamento que a empresa deseja que seu colaborador tenha no caso da utilização da área de transfer.

QUADRO 10

Análise das políticas da instituição pesquisada com base no critério - As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	A política contempla o comportamento que o usuário deve ter, principalmente aqueles que podem utilizar as mídias removíveis e as portas USB. Entretanto trata-se de medidas prescritivas e ainda pouco exploradas, haja vista que caso o usuário se envolva em um incidente da segurança só lhe resta perder o uso das ferramentas. Não são abordados fatores sobre como agir no caso de ser vítima de incidentes de segurança da informação. Paralelamente, no caso da maior parte dos colaboradores que não têm acesso às mídias removíveis e tampouco às portas USB a política não explora forma com que esse funcionário pode contribuir através de seu comportamento para garatir a segurança informacional da empresa.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Conforme dito as condutas ficam restritas a uma abordagem de se executar o que se pede. No caso dessa política de software ativirus isso se restringe a não desistalar o referido software; não abrir arquivos recebidos por e-mail; não baixar conteúdo da internet; Interferir quando o software estiver realizando atualizações e/ou verificações na estação. Podendo ser mais bem explorada por parte da organização e garantir um envolvimento maior dos colaboradores no processo de garantia da segurança da informação organizacional.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Nas políticas analisadas as condutas ficam restritas a uma abordagem de se executar o que se pede. No caso dessa política de uso da internet corporativa, isso se restringe a não acessar os sites que constam no grupo de sites proibidos e usar o acesso da internet para fins de trabalho.

QUADRO 10

Análise das políticas da instituição pesquisada com base no critério - As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	A política instrui o usuário no sentido de preservar a informação da empresa haja vista que não permite o descarte de documentos nos lixos da empresa e tampouco a utilização do material como rascunho.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	A política instrui o usuário acerca da necessidade de um acesso controlado e como obtê-lo. A política também esclarece sobre os tipos de classificação de perímetros e de acesso físico à organização.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Essa política restringe o comportamento do usuário de forma prescritiva. O que a empresa entende que o usuário deve seguir no sentido de acesso remoto à rede de dados e sistemas em produção.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Essa política restringe o comportamento do usuário de forma prescritiva. O que a empresa entende que o usuário deve seguir no sentido de acesso remoto à rede de dados e sistemas em produção.

QUADRO 10

Análise das políticas da instituição pesquisada com base no critério - As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Essa política descreve amplamente quais os comportamentos que a empresa deseja que seus funcionários tenham para garantir a proteção de seus ativos informacionais. Essa abordagem percorre Recomendações quanto à utilização do correio eletrônico corporativo; Sobre a utilização e guarda de senhas de acesso dos softwares da empresa; sobre Informações Pessoais ou Informações confidenciais da organização; sobre abordagem a pessoas desconhecidas; sobre não visitar sites desconhecidos e ler atentamente a URL dos sites que você for "convidado a visitar"; não compartilhar diretórios de sua estação de trabalho com outras pessoas; em caso de comportamento anormal de computador do usuário ele deve procurar o setor especificado na política; não usar documentos impressos que contenham informações relacionadas ao negócio da cooperativa como rascunho; destruir documentos impressos que não se fazem mais úteis ou necessários nas fragmentadoras de papel; não transitar com documentos que contenham informações da empresa fora de envelope ou capa opaca; Caso tenha sido vítima de ataque da Engenharia social, comunicar imediatamente ao setor especificado na política; evitar falar ou conversar a respeito de temas relacionados ao seu trabalho em ambientes públicos tais como táxis, restaurantes, aeroportos ou elevadores; Se o caolaborador suspeitar que alguém obteve sua senha sem o seu conhecimento ou acessou ilicitamente seu computador avisar ao setor especificado na política e solicitar a alteração imediata de sua senha;
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 10

Análise das políticas da instituição pesquisada com base no critério - As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas contemplam qual comportamento o usuário deve ter com relação à segurança da informação.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	A política determina claramente as resposanbilidades, porém, não contemplam detalhadamente as condutas que seus recursos humanos devem ter.
Criação e alteração de login de acessos à rede de dados e sistemas da	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	A política prevê apenas comportamento de acesso à rede de dados e aos sistemas através de login e senha, e, também prescreve a necessidade de se efetivar o logout no fim da utilização destes.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto	A política prevê a necessidade de se passar por algumas diretrizes prescritas na política tais como preenchimento de formulários, termos de sigilo e solicitação de acesso através de login e senha.

QUADRO 11

Análise das políticas da instituição pesquisada com base no critério - Existem indicadores de segurança da informação que são avaliados pela instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem indicadores de segurança da informação que são avaliados pela instituição.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Não se aplica
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Nessa política poderiam estar expressos os indicadores de segurança da informação que fazem parte do processo de gestão da informação e do conhecimento organizacional, como por exemplo, indicadores de segurança da informação para a ferramenta BSC. Não dispõe-se da informação se a organização utiliza ou não critérios de gestão estratégica, mas pela não apresentação desses indicadores nas políticas tem-se a impressão de que a segurança da informação não faz parte da gestão estratégica ou planejamento estratégico da empresa.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Nessa política poderiam estar expressos os indicadores de segurança da informação que fazem parte do processo de gestão da informação e do conhecimento organizacional, como por exemplo, indicadores de segurança da informação para a ferramenta BSC. Não dispõe-se da informação se a organização utiliza ou não critérios de gestão estratégica, mas pela não apresentação desses indicadores nas políticas tem-se a impressão de que a segurança da informação não faz parte da gestão estratégica ou planejamento estratégico da empresa.

QUADRO 11

Análise das políticas da instituição pesquisada com base no critério - Existem indicadores de segurança da informação que são avaliados pela instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem indicadores de segurança da informação que são avaliados pela instituição.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Nessa política também não são apontados indicadores de segurança da informação.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas	Nessa política também não são apontados indicadores de segurança da informação.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Nessa política também não são apontados indicadores de segurança da informação.
Acesso remoto à rede de dados e sistemas em	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Nessa política também não são apontados indicadores de segurança da informação.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Nessa política também não são apontados indicadores de segurança da informação.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Nessa política também não são apontados indicadores de segurança da informação.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 11

Análise das políticas da instituição pesquisada com base no critério - Existem indicadores de segurança da informação que são avaliados pela instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem indicadores de segurança da informação que são avaliados pela instituição.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	A política não menciona indicadores de segurança da informação.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	A política não menciona indicadores de segurança da informação.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	A política não menciona indicadores de segurança da informação.

QUADRO 12

Análise das políticas da instituição pesquisada com base no critério - Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Não se aplica
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Nessa política há referência que caso ocorra algum incidente de segurança da informação o assunto deve ser tratado conforme as diretrizes do termo de responsabilidade e sigilo
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Nessa política entende-se que os incidentes de segurança da informação só serão comunicados aos envolvidos após investigação

QUADRO 12

Análise das políticas da instituição pesquisada com base no critério - Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Nessa política existe uma indicação de responsabilidade direta dos gestores de orientar os colaboradores de sua gestão com relação a tomar conhecimento da utilização adequada dos acessos liberados, sobre os procedimentos de monitoramento adotados pela empresa e as punições previstas aos infratores (das diretrizes da política de segurança da informação); Possíveis invasões e/ou infecções por vírus, softwares maliciosos e etc, causadas pela utilização indevida da Internet; Danos causados à estação de trabalho e/ou a rede de computadores provenientes da utilização indevida da Internet; Ações corretivas quando da ocorrência de problemas oriundos da utilização indevida da Internet. Trata-se de indicações pré ocorrência de algum incidente
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas	Essa política não prevê a comunicação de incidentes ocorridos no descarte de documentos sigilosos aos colaboradores. Pelo que tenho observado a comunicação de incidentes aos colaboradores não parece ser uma prática da organização
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Essa política não prevê a comunicação de incidentes ocorridos no descarte de documentos sigilosos aos colaboradores. Pelo que tenho observado a comunicação de incidentes aos colaboradores não parece ser uma prática da organização

QUADRO 12

Análise das políticas da instituição pesquisada com base no critério - Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Essa política não prevê a comunicação de incidentes caso ocorra acesso remoto à rede de dados e sistemas em produção. Pelo que tenho observado a comunicação de incidentes aos colaboradores não parece ser uma prática da organização
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Essa política não prevê a comunicação de incidentes caso ocorram problemas com os backups estipulados pela organização. Pelo que tem-se observado a comunicação de incidentes aos colaboradores não parece ser uma prática da organização
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Como se trata de uma política de atenução de risco de engenharia social a política deveria prever a comunicação de incidentes ou ataques ocorridos aos colaboradores e incentivar canais de discussão sobre esse assunto, visando a consolidação de atitudes e de um
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 12

Análise das políticas da instituição pesquisada com base no critério - Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe nessa política a indicação sobre a necessidade de se comunicar aos colaboradores os incidentes de segurança da informação ocorridos.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	A política denominada segurança da informação não faz menção a incidentes de segurança e tampouco à comunicaçãode incidentes de segurança
Criação e alteração de login de acessos à rede de dados e sistemas da	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	A política denominada login de acesso à redes e sistemas não faz menção à incidentes de segurança e tampouco à comunicação de incidentes de segurança
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	A política não menciona qual o comprtamento que a empresa deseja que seu colaborador tenha no caso de ocorrência de incidentes de segurança da informação

QUADRO 13

Análise das políticas da instituição pesquisada com base no critério - As especificações das políticas de segurança da informação da instituição são de fácil compreensão (curtas, palavras fáceis, objetivas, boa formatação).

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As especificações das políticas de segurança da informação da instituição são de fácil compreensão (curtas, palavras fáceis, objetivas, boa formatação).
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso as dependências da organização.	A política em questão é de fácil compreensão apesar de não trazer detalhes acerca de que tipo de material a organização se refere
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Política de fácil compreensão apesar de envolver várias etapas desenvolvidas por equipes ou gerencias diferentes. É necessário que o colaborador esteja de posse da política para orientá-lo no cumprimento das determinações da empresa com relação a essa
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Política de fácil compreensão, com sanções claramente expostas e quais são os procedimentos determinados pela empresa para a correta utilização da área "tranfer".
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	As específicações foram redigidas de forma clara e com objetividade. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	As específicações foram redigidas de forma clara e com objetividade. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	As específicações foram redigidas de forma clara e com objetividade. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas

QUADRO 13

Análise das políticas da instituição pesquisada com base no critério - As especificações das políticas de segurança da informação da instituição são de fácil compreensão (curtas, palavras fáceis, objetivas, boa formatação).

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As especificações das políticas de segurança da informação da instituição são de fácil compreensão (curtas, palavras fáceis, objetivas, boa formatação).
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	As específicações foram redigidas de forma clara e com objetividade. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	As específicações foram redigidas de forma clara e com objetividade. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	As específicações foram redigidas de forma clara e com objetividade. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	As específicações foram redigidas de forma clara e com objetividade apesar do uso de um quantidade grande de termos técnicos. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	As específicações foram redigidas de forma clara e com objetividade usando inclusive exemplo do dia-a-dia. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 13

Análise das políticas da instituição pesquisada com base no critério - As especificações das políticas de segurança da informação da instituição são de fácil compreensão (curtas, palavras fáceis, objetivas, boa formatação).

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As especificações das políticas de segurança da informação da instituição são de fácil compreensão (curtas, palavras fáceis, objetivas, boa formatação).
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	As específicações foram redigidas de forma clara e com objetividade usando inclusive exemplo do dia-a-dia. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	As específicações foram redigidas de forma clara e com objetividade usando inclusive exemplo do dia-a-dia. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	As específicações foram redigidas de forma clara e com objetividade usando inclusive exemplo do dia-a-dia. Nota-se que as políticas seguem um padrão de formatação de ajuda na familiarização do usuário com essas políticas

QUADRO 14

Análise das políticas da instituição pesquisada com base no critério - Existe regra expressa na política de segurança da informação para que riscos, ameaças e vulnerabilidades sejam bem documentados.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério:Existe regra expressa na política de segurança da informação para que riscos, ameaças e vulnerabilidades sejam bem
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Essa política não contempla essa referência
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Não há referência nessa política com relação à documentação de incidentes, riscos ameaças e vulnerabilidades que porventura ocorram.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Não há referência nessa política com relação à documentação de incidentes, riscos ameaças e vulnerabilidades que porventura ocorram.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Não há referência nessa política com relação à documentação de incidentes, riscos ameaças e vulnerabilidades que porventura ocorram.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas	Nessa política existe a regra expressa que os documentos devem ser triturados antes de sairem da empresa para, por exemplo, reciclagem.

QUADRO 14

Análise das políticas da instituição pesquisada com base no critério - Existe regra expressa na política de segurança da informação para que riscos, ameaças e vulnerabilidades sejam bem documentados.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério:Existe regra expressa na política de segurança da informação para que riscos, ameaças e vulnerabilidades sejam bem documentados.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Não existe referência nessa política para que riscos, ameaças e vulnerabilidades com relação à segurança física do ambiente de tecnologia sejam documentados.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Não existe referência nessa política para que riscos, ameaças e vulnerabilidades com relação ao acesso remoto à rede de dados e sistemas em produção.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Não existe referência nessa política para que riscos, ameaças e vulnerabilidades com relação aos backups.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Existe referência na política para que arquivos ou potenciais provas de que o colaborador foi atacado não sejam apagados, haja vista que esses dados ou informações podem ser úteis em caso de um eventual processo judicial contra o atacante. Ressalta-se que não existe um documento formal, expresso na política, para documentar riscos,
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 14

Análise das políticas da instituição pesquisada com base no critério - Existe regra expressa na política de segurança da informação para que riscos, ameaças e vulnerabilidades sejam bem documentados.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério:Existe regra expressa na política de segurança da informação para que riscos, ameaças e vulnerabilidades sejam bem documentados.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Na política de segurança da informação não existe referência à documentação de nenhum tipo.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Na política de login de acesso à redes e sistemas não existe referência à documentação de nenhum tipo.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Não há referências na política em questão acerca da necessidade de documentação de nenhum tipo.

QUADRO 15

Análise das políticas da instituição pesquisada com base no critério - Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Uso de formulários de autorização de visitas; Formulários de saída de materiais e equipamentos; Determinações para uso de crachá.
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Formulário de solicitação de visita; Colher aprovação junto à equipe competente; Determinações das ações a serem desenvolvidas com relação ao recebimento de visistas que devem ser executadas por diferentes equipes ou gerentes.
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Existe direcionamento apenas com relação a um termo de responsabilidade e sigilo tido como documento complementar. Nenhum outro mecanismo é relacionado na redação dessa política.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Existe direcionamento com relação ao uso do termo de resposabilidade e sigilo, sobre a necessidade de se comprometer com o Termo de Responsabilidade e Compromisso para utilização de mídia removível e/ou portas USB, e, sobre comunicação formal sobre qual dispositivo foi liberado para uso, no caso, somente mídias removíveis e/ou portas USB.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Essa política se ampara também nas resoluções previstas tanto na política de segurança da informação da empresa quanto na políticas de acesso lógico e segurança Física Do Ambiente De Tecnologia

QUADRO 15

Análise das políticas da instituição pesquisada com base no critério - Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Essa política se ampara também nas resoluções previstas tanto na política de segurança da informação da empresa quanto nas políticas de acesso lógico e segurança Física Do Ambiente De Tecnologia
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas	A política de descarte de documentos é amparada pela política de movimentação de documentos no arquivo geral.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Os mecanismos de execução são descritos na própria política e falam a respeito de acesso restrito, barreiras fisicas, layout físico que evite o acesso do público, controles de acesso, instituição de perímetros de segurança, uso de dispositivos de controle de acesso automatizado, uso de crachás, autorizações, rondas em períodos de inatividade, uso de trancas
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Os mecanismos de execução são solicitação de Serviços à Gestão de Tecnologia da Informação e a validação da GTIN Qualidade em TI e Segurança da Informação, assinatura do Termo de Responsabilidade e Compromisso que referencie essa liberação pelo Gestor de TI e pelo colaborador e/ou prestador de serviço que deve executar os acessos, dando ciência e concordância nas cláusulas do Termo de Responsabilidade e Compromisso.

QUADRO 15

Análise das políticas da instituição pesquisada com base no critério - Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Os mecanismos de execução dessa política são Informações completas sobre as políticas configuradas e identificação das fitas para utilização das unidades de backup que também é chamado de relatório de backup
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Os mecanismos de execução dessa política, além do detalhamento dado ao comportamento que se espera do usuário, são também usadas as políticas de Uso, Criação e Conservação de Senhas; Acesso Lógico; Segurança da Informação e de Visitas à empresa estudada.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 15

Análise das políticas da instituição pesquisada com base no critério - Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem orientações na política organizacional com relação aos mecanismos de execução necessários para que se propicie o cumprimento das políticas de segurança da informação pelos colaboradores.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	O mecanismo de execução claramente evidenciado na política refere-se à criação da área de segurança em tecnologia da informação no departamento de tecnologia da informação que ficará responsável pela implementação, atualização,monitoramento e efetividade da política de segurança da informação.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	O mecanismo de execução do login de lacesso à redes e sistemas é a criação desses parâmetros quando o usuário é admitido, o uso de login login de acesso à redes e sistemas na rotina do usuário e o bloqueio desses dados quando ele é demitido.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Os mecanismos de execução são formulários, termos, solicitações de permissão de acesso e as outras normas que se vinculam a essa como complementares.

QUADRO 16

Análise das políticas da instituição pesquisada com base no critério - Existe orientação na política de segurança informacional para que cada colaborador seja orientado ou obrigado a fazer back-ups diários das informações por ele processadas em um servidor disponibilizado pela instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe orientação na política de segurança informacional para que cada colaborador seja orientado ou obrigado a fazer back-ups diários das informações por ele processadas em um servidor disponibilizado pela instituição.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não se aplica
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada "transfer", visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Não se aplica
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Essa política apesar de permitir o uso de mídias removíveis não informa se esse mecanismo poderia ser utilizado inclusive como um backup adicional. Nota-se que não há orientações nessa política acerca de backup prévio, em um dos servidores da empresa, das informações que estão transitando em mídias removíveis e ou portas
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Nessa política não há orientações acerca de back, acredita-se que, neste caso, não se aplica.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Não existe nessa política orientação acerca back-ups de informações adquiridas através de conteúdo da internet. Como não é possível baixar o conteúdo pesquisado, talvez seja necessário complementar essa política pontuando soluções caso o usuário utilize uma fonte de informação virtual para a tomada de decisão. Nota-se, dependendo da fonte, que a informação adquirida através da internet possa se tornar ativo para a organização

QUADRO 16

Análise das políticas da instituição pesquisada com base no critério - Existe orientação na política de segurança informacional para que cada colaborador seja orientado ou obrigado a fazer back-ups diários das informações por ele processadas em um servidor disponibilizado pela instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe orientação na política de segurança informacional para que cada colaborador seja orientado ou obrigado a fazer back-ups diários das informações por ele processadas em um servidor disponibilizado pela instituição.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	Não se aplica
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Não se aplica
Acesso remoto à rede de dados e sistemas em	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Não há orientações nessa política para que backups daquilo que foi acessado remotamente sejam feitos e a forma que eles devam ser
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Essa política prevê várias orientações com relação aos procedimentos de backup em vigor na organização. Conforme dito anteriormente esse backup majoritariamente ocorre de forma automática com dia e hora determinados. Nota-se que existe determinação indicando que os backups não são realizados nos
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Não se aplica
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 16

Análise das políticas da instituição pesquisada com base no critério - Existe orientação na política de segurança informacional para que cada colaborador seja orientado ou obrigado a fazer back-ups diários das informações por ele processadas em um servidor disponibilizado pela instituição.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existe orientação na política de segurança informacional para que cada colaborador seja orientado ou obrigado a fazer back-ups diários das informações por ele processadas em um servidor disponibilizado pela instituição.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Nessa política de segurança da informação não há referências a back up.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Existe orientação no sentido de fazer back-ups caso haja uma alteração de login de usuário.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	No quesito de suspensão de direito de acesso seja ele por quaisquer motivações, não contempla o back up das informações processadas pelo usuário que perderá o acesso.

QUADRO 17

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação são volumosas e de cumprimento inviável.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação são volumosas e de cumprimento inviável.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Política de fácil compreensão apesar de envolver várias etapas desenvolvidas por equipes ou gerências diferentes. É necessário que o colaborador esteja de posse da política para orientá-lo no cumprimento das determinações da empresa com relação a essa norma.
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Política de fácil compreensão, não volumosa e de cumprimento viável.

QUADRO 17

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação são volumosas e de cumprimento inviável.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação são volumosas e de cumprimento inviável.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Política de fácil compreensão, não volumosa e de cumprimento viável.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 17

Análise das políticas da instituição pesquisada com base no critério - As políticas de segurança da informação são volumosas e de cumprimento inviável.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas de segurança da informação são volumosas e de cumprimento inviável.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Criação e alteração de login de acessos à rede de dados e sistemas da	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Política de fácil compreensão, não volumosa e de cumprimento viável.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Política de fácil compreensão, não volumosa e de cumprimento viável.

QUADRO 18

Análise das políticas da instituição pesquisada com base no critério -As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do colaborador.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não se aplica.
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Existe um check list de atividades que devem ser cumpridas por cada gerência para preparação da visita
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Essa política não contempla um check list mas a necessidade de limpeza dos dados que passam pela área de transfer apenas por tempo determinado
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Essa política dispõe de um roteiro que deve ser cumprido caso o colaborador necessite de acesso às mídias removíveis e ou portas USB. Entretanto não existe um chek-list previsto na política que pode ser utilizado pelo colaborador no sentido de saber se ele está tendo acesso somente àquilo que ele solicitou para não ser resposabilizado depois. Outro ponto é que o colaborador pode ser parceiro do setor de controle quando ele for instruido a sempre se reconectar com seu usuário e senha após uma intervenção do setor de tecnologia da informação, a seguir um check list para verificar se ele (colaborador) dispõe de algum acesso indevido que depois venha a ser penalizado por isso.

QUADRO 18

Análise das políticas da instituição pesquisada com base no critério -As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do colaborador.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do colaborador.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Essa política não dispõe de um check list de segurança da informação que deve ser realizado pelo colaborador. Pelo descrito, acredita-se que a empresa ficará responsável por fazer as atualizações, remoções, instalações e verificações necessárias no que concerne ao software antivirus remota e automaticamente.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Não existe, nessa política, um check list que deve ser cumprido diariamente pelo colaborador. Existem apenas apenas orientações acerca do tipo de conteúdo que não pode ser acessado.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a	O check list de segurança da informação se dá a partir do cumprimento do ckeck list de descarte consciente da documentação.
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a	Sim existe um procedimento de controle de acesso que deve ser seguido por todos os colaboradores

QUADRO 18

Análise das políticas da instituição pesquisada com base no critério -As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do colaborador.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do colaborador.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Não há um check list que o colaborador deva cumprir imediatamente antes de acessar remotamente a empresa. Acredita-se que indicações comportamentais, como por exemplo, análise do local onde o colaborador ou parceiro se encontram para realizar o acesso, ou, que os acessos devam acontecer quando o colaborador estiver sozinho ou não usar máquinas e equipamentos de *lan houses* para efetivar acesso remoto etc.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	Não existe um checklist diário que deve ser cumprido por cada colaborador haja vista que os procedimentos dessa política são majoritariamente automáticos. Para os procedimentos que envolvem o pessoal de tecnologia da informação existe um relatório de backup que
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Não existe um check list apenas orientações para um comportamento seguro.
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 18

Análise das políticas da instituição pesquisada com base no critério -As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do colaborador.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: As políticas prevêem a necessidade de se cumprir um check list de segurança da informação nas atividades do dia-a-dia do colaborador.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Não há referências sobre check-lists nessa política.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Não há referências sobre check-lists nessa política
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto	Há uma prescrição de sequência de formulários e termos que devem ser assinados antes de solicitado o acesso. Nota-se porém que essas prescrição não estão em formato de check-list.

QUADRO 19

Análise das políticas da instituição pesquisada com base no critério - Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação previstas nas políticas de segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação previstas nas políticas de segurança da informação.
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Não são observadas sanções ou recompensas no caso de cumprimento ou não dessa política
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	Não são observadas sanções ou recompensas no caso de cumprimento ou não dessa política
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Essa política determina ao usuário quais são as sanções que incorrerão junto àqueles que infringirem essa regra.
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Essa política determina ao usuário quais são as sanções que incorrerão junto àqueles que infringirem essa regra.
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	Presença de sanções caso o usuário não cumpra com as deliberações previstas. Bonificações ausentes.
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Presença de sanções caso o usuário não cumpra com as deliberações previstas. Bonificações ausentes.

QUADRO 19

Análise das políticas da instituição pesquisada com base no critério - Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação previstas nas políticas de segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação previstas nas políticas de segurança da informação.
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	Não existem sansções e nem recompensas previstas na política
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Não existem sansções e nem recompensas previstas na política
Acesso remoto à rede de dados e sistemas em	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	Existem sanções caso, através da auditoria, sejam confirmados casos de não cumprimento das diretrizes dispostas na política em
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	A política em questão não prevê sanções e nem recompensas
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	A política em questão não prevê sanções e nem recompensas
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica.

QUADRO 19

Análise das políticas da instituição pesquisada com base no critério - Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação previstas nas políticas de segurança da informação.

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação previstas nas políticas de segurança da informação.
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Não há referências sobre recompensas ou punições nessa política.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Não há referências sobre recompensas ou punições nessa política
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Não há referências sobre recompensas ou punições nessa política

QUADRO 20

Análise das políticas da instituição pesquisada com base no critério - Controle expresso nas políticas de acesso para entrada e/ou saída de recursos humanos, dados e informações em formato digital ou físico e/ou recursos físicos pertencentes à organização

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Controle expresso nas políticas de acesso para entrada e/ou saída de recursos humanos, dados e informações em formato digital ou físico e/ou recursos físicos pertencentes à organização
Controle de acesso às dependências da instituição pesquisada	Definir os critérios e procedimentos para o controle de acesso às dependências da organização.	Essa política prevê os critérios para entrada de recursos humanos na empresa. Há uma relação sobre materiais na política, entretando não deixa claro detalhes sobre este. Nota-se que não há uma referência direta e clara com relação à saída de informações da organização.
Visitas à empresa pesquisada	Estabelecer critérios para assegurar a eficaz recepção a visitantes na empresa.	As normas com relação às visitas que são objeto dessa política também podem ser considerados como um tipo de controle de acesso às dependências da empresa.
Utilização da área de transferência	Regularizar a utilização da área de transferência da rede de dados da instituição pesquisada, atualmente denominada “transfer”, visando manter a confidencialidade e disponibilidade das informações armazenadas nesta área.	Não se aplica
Utilização de mídias removíveis e ou portas USB	Regular a utilização de dispositivos acionadores de mídias removíveis e portas USB nas estações de trabalho existentes na instituição pesquisada.	Essa política não deixa claro quais são os critérios para saída de informações da empresa. Paralelamente não faz referência sobre nenhuma outra política que poderia regular tal quesito. Nota-se que não há uma orientação direta e clara com relação à saída e compartilhamento de informações que transitam em mídias removíveis
Sofware Antivirus	Regular a instalação, manutenção, atualização e utilização do software antivírus nos servidores e estações de trabalho que ingressem na rede de computadores da instituição pesquisada.	No caso da política de software antivirus esse critério não se aplica
Utilização da Internet corporativa	Regular a utilização da Internet em toda a empresa	Controle presente no sentido de não ser permitido o download de arquivos advindos de e-mail ou de conteúdo da internet. Além da presença do controle, as auditorias ratificam a necessidade de seguir essas diretrizes propostas.

QUADRO 20

Análise das políticas da instituição pesquisada com base no critério - Controle expresso nas políticas de acesso para entrada e/ou saída de recursos humanos, dados e informações em formato digital ou físico e/ou recursos físicos pertencentes à organização

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Controle expresso nas políticas de acesso para entrada e/ou saída de recursos humanos, dados e informações em formato digital ou físico e/ou recursos físicos pertencentes à organização
Descarte de documentos impressos	Estabelecer o procedimento para descarte de documentos impressos da organização que não tenham mais utilidade em função de vencimento de prazo de validade, obsolescência das informações, não havendo motivos para permanência em formato impresso, e caso a manutenção desse formato impresso coloque em risco a confidencialidade de suas informações.	Controle de saída de documentos contendo informações sigilosas apenas triturados
Segurança Física do Ambiente de Tecnologia	Definir os mecanismos de controle de acesso às instalações da Gestão de Tecnologia da Informação da instituição, assim como definir procedimentos relativos a esses acessos.	Controle detalhado de acesso de recursos humanos na organização com mecanismos de execução definidos.
Acesso remoto à rede de dados e sistemas em produção	Regular o acesso remoto à rede de dados, aos sistemas em produção e ao ambiente de desenvolvimento de sistemas.	A política não faz referência a colaboradores que utilizam o acesso remoto através de máquinas e equipamentos como por exemplo notebooks, smartphones e tablets que pertençam à organização.
Backups	Definir os critérios de realização do processo de backup de dados dos servidores da instituição	A política não faz referência sobre a necessidade de saída de máquinas e equipamentos da empresa desde que tenham passado pelo processo de backup previamente.
Atenuação de risco de engenharia social	Orientar os colaboradores da empresa, na adoção de práticas que os auxiliem na atenuação do risco representado pela prática de engenharia social.	Não se aplica
Utilização do correio eletrônico corporativo	Instruir e regular a correta utilização do correio eletrônico corporativo, em conformidade com a legislação e Política de Segurança da Informação da instituição pesquisada.	Não se aplica

QUADRO 20

Análise das políticas da instituição pesquisada com base no critério - Controle expresso nas políticas de acesso para entrada e/ou saída de recursos humanos, dados e informações em formato digital ou físico e/ou recursos físicos pertencentes à organização

Políticas da Instituição:	Objetivos das Políticas da Instituição Pesquisada:	Análise do critério baseado na revisão de literatura: Critério: Controle expresso nas políticas de acesso para entrada e/ou saída de recursos humanos, dados e informações em formato digital ou físico e/ou recursos físicos pertencentes à organização
Segurança da Informação	Assegurar à empresa a conformidade da Política de Segurança da Informação com as normas pertinentes, visando proteger os dados, garantindo que as informações que integram o patrimônio da organização e aquelas sob sua guarda, assim como as ferramentas utilizadas para sua obtenção, geração, modificação, armazenagem e disponibilização estejam em conformidade com as leis brasileiras e com as regras que regem o Sistema de Saúde Suplementar do Brasil, assim como dos Conselhos Federal e Regional de Medicina e da ANS – Agência Nacional de Saúde Suplementar. Manter os processos apoiados pelos sistemas informatizados da corporação através da prevenção e solução de eventos de quebra de segurança da Informação.	Existe uma referência clara sobre a necessidade de proteção ao patrimônio de informações da empresa em questão. Contudo, não há menção nessa política sobre formas de controle de entrada e\ou saída de recursos de quaisquer tipos pertencentes à empresa.
Criação e alteração de login de acessos à rede de dados e sistemas da empresa	Definir os critérios para a criação e alteração de login para acesso à rede de dados e sistemas da empresa.	Há discrimição na política para acesso aos sistemas e redes de acesso somente através de login desenvolvido pela gerência de tecnologia da informação.
Acesso lógico	Regular o acesso lógico às informações, aos ativos de processamento e aos ativos de informação da instituição, bem como atribuir as responsabilidades a seus colaboradores, conselheiros, cooperados, terceiros/prestadores, clientes e fornecedores enquanto detentores destes direitos de acesso.	Controle de acesso aos ativos informacionais através de login e senha

A análise a seguir parte, primeiramente, da tentativa de elucidar parte dos objetivos específicos da pesquisa citados no início dessa seção.

A análise das políticas da instituição nos faz perceber um forte posicionamento tecnicamente orientado. Destaca-se simultaneamente que vários critérios de avaliação que foram levantados na revisão de literatura são inexplorados ou pouco explorados pela instituição. Este fator nos faz perceber o quanto a abordagem sistêmica, holística e equitativa para os elementos *pessoas, processos* e *tecnologias* ainda demanda desenvolvimento nesse ambiente organizacional. Essa constatação nos faz perceber que, quando existe uma tendência a uma abordagem tecnicamente orientada, os usuários da informação vêem nas tecnologias a única forma, ou a forma mais segura e completa de evitar incidentes de segurança da informação. E essa é uma vertente perigosa, pois os elementos *pessoas, processos* e *tecnologias* ficam desconectados perante esse usuário e ele passa a acreditar que a tecnologia isoladamente resolverá a maior parte dos casos de incidentes de segurança informacional que, porventura, ocorram na instituição.

Doravante, observa-se que existe um campo aberto e que necessita de desenvolvimento no que concerne às ações juntos às pessoas, para que elas se sintam agentes promotores e desenvolvedores da segurança da informação; a solidificação sistêmica das políticas de informação para que elas sejam fonte de informação para amparar e direcionar os colaboradores na maior variedade possível de especificações, aplicações e casos; e a tecnologia como ferramenta que garantirá, apoiada nos processos e nas pessoas, maior segurança aos ativos informacionais corporativos.

No que concerne ao objetivo geral da pesquisa, a fase de análise das políticas contribui para detectar que existe abertura para que incidentes de segurança da informação ocorram. Isso se deve ao fato de que na instituição pesquisada, existem poucas ações que preparem os recursos humanos para não se envolverem em circunstâncias que possam gerar falhas de segurança da informação.

Outro ponto é que a análise das políticas propicia, ainda, entendimento de parte do objetivo específico da pesquisa, que é compreender em que medida estaria esse usuário da informação corporativa preparado e amparado para evitar falhas de segurança. Essa compreensão, acredita-se, que pode ser obtida através da análise dos aspectos presentes na revisão de literatura e ausentes na análise das políticas. Nesse sentido, pode-se citar, primordialmente, que as políticas de segurança da informação não são exploradas pela organização no sentido de promover a melhoria contínua dos

processos e o desenvolvimento do conhecimento corporativo. O usuário é parte responsável pela segurança da informação da empresa somente em alguns casos, sendo que, na maior parte deles, a área de tecnologia aparece como maior provedor de segurança da informação. Nas políticas de segurança da informação, não há referência desta no planejamento estratégico da organização e também nenhum indicador de segurança da informação previsto nas políticas, fato este que demonstra que a segurança da informação não faz parte do negócio da empresa. Na maior parte dos casos, observa-se que a empresa não possui uma cultura de prevenir, detectar e documentar incidentes de segurança, nesse sentido as políticas não prevêem que os colaboradores comuniquem à instituição e aos colegas incidentes ocorridos e a ação desse funcionário.

5.2 – Instrumento de coleta de dados

O questionário foi estruturado em duas partes. A primeira, com o objetivo de obter o perfil do entrevistado, com relação ao sexo e escolaridade. A segunda parte, composta por 49 questões, seguiu uma estrutura matricial com uma escala tipo Likert com 4 pontos, sem ponto neutro, sendo os extremos: “Discordo totalmente” (1) e “Concordo totalmente” (4). É importante salientar, que neste trabalho, optou-se por trabalhar com 4 itens. A escala utilizada, segundo categorização de Malhotra (2012) pode ser classificada como balanceada, pois apresenta número igual de categorias favoráveis e desfavoráveis, e forçada, pois os entrevistados foram forçados a emitir uma opinião, não havendo a posição neutra. Para cada afirmativa, o respondente tinha necessariamente que discordar ou concordar.

Conforme descrito na metodologia de pesquisa, a seguir relacionam-se todas as afirmações negativas do instrumento de coleta de dados. São elas:

- Afirmativa 4: A segurança da informação na instituição na qual trabalho é responsabilidade apenas do setor de tecnologia da informação.
- Afirmativa 7: Na minha percepção, a instituição investe mais em tecnologia para assegurar a segurança da informação corporativa e menos em treinamentos para as pessoas, sobre segurança da informação e em políticas de segurança da informação.

- Afirmativa 34: A instituição permite que eu acesse a rede corporativa, grave dados em pen-drives, CD´s, DVD´s e/ou imprima informações para uso, tanto no ambiente institucional, quanto em casa.
- Afirmativa 36: No ambiente corporativo eu tenho acesso irrestrito a todos os sites que precisar ou quiser consultar.
- Afirmativa 37: No ambiente institucional posso escolher quais itens das políticas de segurança da informação vou cumprir.
- Afirmativa 43: Sinto vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é a segurança da informação de minha instituição.

Com relação ao pré-teste, o procedimento foi executado junto aos alunos da pós-graduação em Ciência da Informação. Solicitou-se a 20 alunos que respondessem ao questionário para verificar possíveis dificuldades de entendimento do questionário, ou mesmo de funcionamento do site onde o questionário foi disponibilizado. Nenhum erro ou dificuldade foram encontrados pelos respondentes. Assim, procedeu-se com o envio da pesquisa à instituição pesquisada.

5.2.1 – Implementação da metodologia para análise dos dados: Tabulação dos dados do questionário

De posse dos dados da pesquisa aplicada, procede-se com a organização dos dados, para que se proceda com a análise dos dados primários.

Primeiramente, foi feita a tabulação e, na sequência, o agrupamento dos dados obtidos em três arenas – *Pessoas, Processos e Tecnologia*.

Os dados são tabulados conforme tabela abaixo:

TABELA 1

Instrumento de coleta de dados

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
1	Qual seu sexo?	0	0	0	0
2	Qual é a sua escolaridade?	0	0	2	0
3	Você entende o que é segurança da informação	28	7	0	0
4	A segurança da informação na instituição na qual trabalho é responsabilidade apenas do setor de tecnologia da informação.	6	9	6	14
5	Você, dentro de suas atribuições e funções no dia-a-dia, se sente parte responsável pela segurança da informação praticada na instituição?	29	6	0	0
6	A partir das diretrizes que a instituição fornece sobre como agir seguramente, eu consigo entender como atuar e agir de modo a garantir a confidencialidade, disponibilidade e a integralidade dos dados com os quais trabalho.	9	21	3	2
7	Na minha percepção, a instituição investe mais em tecnologia para assegurar a segurança da informação corporativa e menos em treinamentos para as pessoas sobre segurança da informação e em políticas de segurança da informação.	14	14	5	2
8	Percebo que a instituição empreende e explora as ações de segurança da informação para, através delas, promover a melhoria continua dos processos institucionais.	5	14	13	3
9	Eu poderia dizer que as ações de segurança da informação em minha instituição geram conhecimento e promovem o aprendizado entre os colaboradores?	2	15	8	9
10	Frequentemente ocorrem interações sociais entre os colaboradores para discutir temas sobre segurança da informação.	0	3	7	25
11	Eu poderia dizer que a segurança da informação na instituição na qual trabalho faz parte do planejamento estratégico ou da gestão estratégica da empresa.	4	14	12	5
12	O desenvolvimento da segurança da informação na instituição na qual trabalho inclui proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo, sejam elas internas e/ou externas à organização.	7	21	5	2

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
13	Quando ocorre um incidente de segurança da informação na instituição, esse incidente é detectado, prevenido e documentado.	5	11	16	3
14	Estão claras as condutas que a instituição deseja que eu tenha com relação à segurança da informação? Como exemplo podemos citar a comunicação de incidentes de segurança.	2	15	11	7
15	Você fica ciente de todas as atualizações de avaliação de riscos de seu departamento, setor ou área?	5	10	9	11
16	Há ocorrência de auditorias sobre segurança da informação no seu departamento ou setor ou área?	8	12	10	5
17	Você sabe quem são as pessoas responsáveis pela segurança da informação na sua instituição?	18	11	1	5
18	Há instruções e políticas formais em sua instituição que ensinam como a empresa espera que você aja com relação à segurança da informação.	7	13	7	8
19	Há indicadores de segurança da informação que são avaliados pela instituição na qual trabalho.	2	14	11	8
20	Há indicadores de segurança da informação que são avaliados pelo setor / departamento no qual trabalho.	2	15	9	9
21	A instituição comunica aos colaboradores sobre os incidentes de segurança da informação ocorridos.	1	7	6	21
22	Conheço os procedimentos e políticas de segurança da informação adotadas pela instituição na qual trabalho.	4	15	10	6
23	Posso identificar as atuais medidas que estão sendo tomadas em relação à segurança informacional na instituição na qual trabalho.	5	12	13	5
24	Costumo conversar com colegas sobre incidentes de segurança da informação ocorridos comigo ou que tenham ocorrido com eles ou com alguém que conheçamos.	6	12	8	9
25	Tenho oportunidade de sugerir ações de segurança da informação na instituição na qual trabalho.	10	10	4	11
26	As especificações das políticas de segurança da informação da instituição na qual trabalho são de fácil compreensão.	6	14	11	4
27	Os riscos, ameaças e vulnerabilidades com relação à segurança da informação de minha organização são bem documentados.	1	10	16	8
28	Os riscos, ameaças e vulnerabilidades com relação à segurança das informações da organização na qual trabalho são devidamente comunicados aos colaboradores.	2	11	11	11

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
29	Analisando as políticas de informação da organização na qual trabalho, eu diria que elas são efetivas e suficientes para garantir a confidencialidade, integridade e disponibilidade das informações (principalmente das informações sigilosas).	4	16	8	7
30	Através das regras de segurança da informação disponibilizadas por minha organização, eu consigo entender qual deve ser o seu comportamento e como a empresa espera que eu aja com relação à segurança da informação.	5	12	12	6
31	Na minha instituição existem mecanismos de execução que propiciam o cumprimento das políticas de segurança da informação pelos colaboradores.	4	17	12	2
32	Eu sou orientado ou obrigado a fazer back-ups diários das informações por mim processadas em um servidor disponibilizado pela instituição.	4	5	8	18
33	Eu observo, ao utilizar o meu e-mail corporativo, que ocorre a supressão de mensagens que possuem anexos não solicitados.	18	10	3	3
34	A instituição permite que eu acesse a rede corporativa, grave dados em pen-drives, CD´s, DVD´s e/ou imprima informações para uso tanto no ambiente institucional quanto em casa.	3	3	8	20
35	Posso dizer que há envolvimento e apoio das gerências, diretorias e presidência no que concerne às ações se segurança da informação.	5	21	3	4
36	No ambiente corporativo eu tenho acesso irrestrito a todos os sites que precisar ou quiser consultar.	3	4	8	20
37	No ambiente institucional posso escolher quais itens das políticas de segurança da informação vou cumprir.	1	3	8	23
38	Altero mensalmente minhas senhas de acesso aos recursos corporativos (por exemplo: redes, computadores, mídias removíveis etc.).	10	13	7	5
39	Considero volumosa demais a quantidade de diretrizes, normas e procedimentos que devo cumprir.	0	8	17	10
40	Normalmente, acesso os sistemas de informação corporativos de minha casa (acesso remoto) para resolver algum problema ou atender a alguma demanda.	1	7	7	19
41	Posto em redes sociais fatos ou ocorrências que aconteceram na organização ou no meu setor para alertar amigos.	2	1	1	30

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
42	Existe um check list de segurança da informação que devo seguir no meu dia-a-dia.	1	7	7	20
43	Sinto vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é segurança da informação de minha instituição.	1	2	3	28
44	Você poderia dizer que em primeiro lugar você dedica atenção à sua profissão e à especialidade do computador no qual trabalha para depois absorver os valores, missão e visão da empresa para a qual trabalha.	2	10	15	8
45	Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação propostas pela instituição.	2	6	3	24
46	Sou treinado para ter um comportamento seguro.	4	8	6	17
47	Sei com clareza qual é o meu papel na segurança informacional da empresa.	9	10	12	4
48	Existem, na instituição na qual trabalho, programas de educação para formar pessoas com relação à segurança da informação.	2	6	11	16
49	As ameaças de segurança da informação que sofro determinam meu comportamento frente às situações que vivencio.	9	15	6	5
50	Avaliando a situação atual, sinto que o ambiente da empresa é seguro no que concerne às informações que nele são processadas.	7	15	7	5
51	A alta carga de trabalho vinculada à minha atividade prejudica minha percepção e ação com relação à segurança da informação.	5	15	9	6

Já com relação ao agrupamento das questões do instrumento de coleta de dados, tem-se a seguinte seletiva disponibilizada abaixo.

O grupo “Pessoas” é formado por 22 questões, “Processos” por 18 e “Tecnologia” por 9 questões. Não existe um número uniforme de questões para cada arena porque não há possibilidade de diminuir o número que perguntas que compõe cada arena pessoas e se as demais arenas fossem acompanhar a quantidade de questões de pessoas o questionário ficaria demasiadamente grande e poderia prejudicar a coleta dos dados. Paralelamente, o objetivo da pesquisa é investigar a inter-relação entre o elemento humano e a segurança da informação no contexto corporativo, essa prerrogativa já anuncia uma exploração maior da arena *pessoas* em detrimento das demais.

TABELA 2

Agrupamento das perguntas ns arenas: pessoas, processos e tecnologia

	Perguntas do Questionário	Pessoas	Processos	Tecnologia
1	Qual seu sexo?			
2	Qual é a sua escolaridade?			
3	Você entende o que é segurança da informação	x		
4	A segurança da informação na instituição na qual trabalho é responsabilidade apenas do setor de tecnologia da informação.			x
5	Você, dentro de suas atribuições e funções no dia-a-dia, se sente parte responsável pela segurança da informação praticada na instituição?	x		
6	A partir das diretrizes que a instituição fornece sobre como agir seguramente, eu consigo entender como atuar e agir de modo a garantir a confidencialidade, disponibilidade e a integralidade dos dados com os quais trabalho.	x		
7	Na minha percepção, a instituição investe mais em tecnologia para assegurar a segurança da informação corporativa e menos em treinamentos para as pessoas sobre segurança da informação e em políticas de segurança da informação.	x		
8	Percebo que a instituição empreende e explora as ações de segurança da informação para, através delas, promover a melhoria continua dos processos institucionais.		x	
9	Eu poderia dizer que as ações de segurança da informação em minha instituição geram conhecimento e promovem o aprendizado entre os colaboradores?	x		
10	Frequentemente ocorrem interações sociais entre os colaboradores para discutir temas sobre segurança da informação.	x		
11	Eu poderia dizer que a segurança da informação na instituição na qual trabalho faz parte do planejamento estratégico ou da gestão estratégica da empresa.		x	
12	O desenvolvimento da segurança da informação na instituição na qual trabalho inclui proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo, sejam elas internas e/ou externas à organização.			x

	Perguntas do Questionário	Pessoas	Processos	Tecnologia
13	Quando ocorre um incidente de segurança da informação na instituição, esse incidente é detectado, prevenido e documentado.		x	
14	Estão claras as condutas que a instituição deseja que eu tenha com relação à segurança da informação? Como exemplo podemos citar a comunicação de incidentes de segurança.		x	
15	Você fica ciente de todas as atualizações de avaliação de riscos de seu departamento, setor ou área?	x		
16	Há ocorrência de auditorias sobre segurança da informação no seu departamento ou setor ou área?		x	
17	Você sabe quem são as pessoas responsáveis pela segurança da informação na sua instituição?	x		
18	Há instruções e políticas formais em sua instituição que ensinam como a empresa espera que você aja com relação à segurança da informação.		x	
19	Há indicadores de segurança da informação que são avaliados pela instituição na qual trabalho.		x	
20	Há indicadores de segurança da informação que são avaliados pelo setor / departamento no qual trabalho.		x	
21	A instituição comunica aos colaboradores sobre os incidentes de segurança da informação ocorridos.		x	
22	Conheço os procedimentos e políticas de segurança da informação adotadas pela instituição na qual trabalho.	x		
23	Posso identificar as atuais medidas que estão sendo tomadas em relação à segurança informacional na instituição na qual trabalho.		x	
24	Costumo conversar com colegas sobre incidentes de segurança da informação ocorridos comigo ou que tenham ocorrido com eles ou com alguém que conheçamos.	x		
25	Tenho oportunidade de sugerir ações de segurança da informação na instituição na qual trabalho.	x		
26	As especificações das políticas de segurança da informação da instituição na qual trabalho são de fácil compreensão.		x	
27	Os riscos, ameaças e vulnerabilidades com relação à segurança da informação de minha organização são bem documentados.		x	
28	Os riscos, ameaças e vulnerabilidades com relação à segurança das informações da organização na qual trabalho são devidamente comunicados aos colaboradores.		x	

	Perguntas do Questionário	Pessoas	Processos	Tecnologia
29	Analisando as políticas de informação da organização na qual trabalho, eu diria que elas são efetivas e suficientes para garantir a confidencialidade, integridade e disponibilidade das informações (principalmente das informações sigilosas).		x	
30	Através das regras de segurança da informação disponibilizadas por minha organização, eu consigo entender qual deve ser o seu comportamento e como a empresa espera que eu aja com relação à segurança da informação.	x		
31	Na minha instituição existem mecanismos de execução que propiciam o cumprimento das políticas de segurança da informação pelos colaboradores.		x	
32	Eu sou orientado ou obrigado a fazer back-ups diários das informações por mim processadas em um servidor disponibilizado pela instituição.			x
33	Eu observo, ao utilizar o meu e-mail corporativo, que ocorre a supressão de mensagens que possuem anexos não solicitados.			x
34	A instituição permite que eu acesse a rede corporativa, grave dados em pen-drives, CD´s, DVD´s e/ou imprima informações para uso tanto no ambiente institucional quanto em casa.			x
35	Posso dizer que há envolvimento e apoio das gerências, diretorias e presidência no que concerne às ações se segurança da informação.	x		
36	No ambiente corporativo eu tenho acesso irrestrito a todos os sites que precisar ou quiser consultar.			x
37	No ambiente institucional posso escolher quais itens das políticas de segurança da informação vou cumprir.		x	
38	Altero mensalmente minhas senhas de acesso aos recursos corporativos (por exemplo: redes, computadores, mídias removíveis etc.).			x
39	Considero volumosa demais a quantidade de diretrizes, normas e procedimentos que devo cumprir.		x	
40	Normalmente, acesso os sistemas de informação corporativos de minha casa (acesso remoto) para resolver algum problema ou atender a alguma demanda.			x
41	Posto em redes sociais fatos ou ocorrências que aconteceram na organização ou no meu setor para alertar amigos.	x		

	Perguntas do Questionário	Pessoas	Processos	Tecnologia
42	Existe um check list de segurança da informação que devo seguir no meu dia-a-dia.			x
43	Sinto vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é segurança da informação de minha instituição.	x		
44	Você poderia dizer que em primeiro lugar você dedica atenção à sua profissão e à especialidade do computador no qual trabalha para depois absorver os valores, missão e visão da empresa para a qual trabalha.	x		
45	Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação propostas pela instituição.		x	
46	Sou treinado para ter um comportamento seguro.	x		
47	Sei com clareza qual é o meu papel na segurança informacional da empresa.	x		
48	Existem, na instituição na qual trabalho, programas de educação para formar pessoas com relação à segurança da informação.	x		
49	As ameaças de segurança da informação que sofro determinam meu comportamento frente às situações que vivencio.	x		
50	Avaliando a situação atual, sinto que o ambiente da empresa é seguro no que concerne às informações que nele são processadas.	x		
51	A alta carga de trabalho vinculada à minha atividade prejudica minha percepção e ação com relação à segurança da informação.	x		

5.3 – Validação do Instrumento de coleta de dados

A validação do instrumento de coleta de dados seguirá as etapas descritas na metodologia. Para que essa fase privilegie o acompanhamento do leitor frente àquilo que foi proposto e o realizado, optou-se por itemizar as etapas de validação.

5.3.1 – Validação Nomológica ou de conteúdo

Conforme descrito na metodologia, essa pesquisa utilizará a validação nomológica ou de conteúdo para com ferramenta que verifica a evidência superficial da integridade da medida que o instrumento se propõe a mensurar.

Assim, a validade de conteúdo ou validade nominal segundo Malhotra (2012, p.231) pode ser feita pelo pesquisador de forma subjetiva e sistemática para avaliar a representatividade do conteúdo de uma escala para o trabalho de mensuração. O pesquisador escolhido foi o Professor Doutor Maurício Barcellos Almeida da Escola de Ciência da Informação da Universidade Federal de Minas Gerais e pesquisador da temática segurança da informação.

Foi selecionado da literatura da pesquisa um conjunto de variáveis para se trabalhar. Entretanto, como não foi possível trabalhar com todas as variáveis, haja vista que se tratava de agrupamento extenso, houve um reagrupamento privilegiando as variáveis principais segundo julgamento dos autores da pesquisa.

Nesse agrupamento foram reunidas 100 variáveis, retiradas da revisão de literatura do trabalho de vários autores, que comporiam cada uma, uma afirmativa da escala de Likert. Entretanto essa classificação continuou extensa e, a partir de uma nova análise feita pelos pesquisadores, esse número foi reduzido para 49 variáveis, compondo um total de 49 afirmativas do instrumento de coleta de dados.

Essa redução ocorreu através de agrupamento de cada uma das 100 variáveis em arenas – *pessoas, processos* e *tecnologias*. Posteriormente, cada variável foi analisada isoladamente e no conjunto as variáveis semelhantes foram excluídas e as que restaram foram analisadas e apuradas, chegando a um total de 49 variáveis, conforme dito anteriormente. As duas perguntas restantes para totalizar 51 perguntas são questões de abertura não relativas à temática segurança da informação.

Através desse procedimento de análise e da presença de um especialista da área de segurança da informação configurou-se a validação nomológica do questionário. Segundo Hair (2009) essa é uma etapa imprescindível no processo de validação de um instrumento de coleta de dados.

5.3.2 – Confiabilidade

O valor encontrado para as 49 afirmativas do alfa de *Cronbach* foi de 0,937.
Ao avaliar os dados de cada agrupamento obteve-se os seguintes resultados:

- Pessoas: formado por 22 afirmativas, apresentou valor de alfa de *Cronbach* de 0,810.
- Processos: formado por 18 afirmativas, apresentou valor de alfa de *Cronbach* de 0,907.
- Tecnologia: composta por 9 afirmativas, apresentou valor de alfa de *Cronbach* de 0,371.

Nota-se, a partir desses dados, que apenas a arena *tecnologia* obteve valor do alfa da *Cronbach* abaixo do aceitável na pesquisa exploratória, que é de 0,6. A partir desse resultado, decidiu-se utilizar a análise de correlação ítem-total, que também é uma medida de confiabilidade do questionário, com o objetivo de medir a correlação de cada ítem do instrumento de coleta de dados com o escore da escala múltipla. Isso quer dizer que teríamos mais uma forma de medida para validar a confiabilidade do instrumento de coleta de dados. Outro ponto é que, através da análise de correlação item-total, pode-se reduzir as variáveis que agregam pouca informação ao pesquisador e, consequentemente, o número de questões do instrumento de coleta de dados, tendo ao final um questionário mais enxuto e com a mesma capacidade de mensuração.

A medida de confiabilidade correlação item-total, proposta por Hair (2009), é a correlação do item com o escore da escala múltipla, cujo valor deve exceder 0,50.

O coeficiente item-total mostra o coeficiente de correlação de Pearson (r) entre o item específico e o indicador total. Uma menor correlação com o indicador total indica uma maior disparidade do item com as outras medidas tomadas em conjunto. Segundo Pereira (2006):

> Quando o pesquisador estiver criando um indicador para futuras aplicações e não apenas concebendo uma estratégia de redução de dimensionalidade para a análise de seus dados presentes, ele dará particular importância a essa informação (...) mais do que considerar a consistência da medida pelo indicador, o pesquisador estará verificando se a contribuição de cada item é efetiva o suficiente para valer o esforço de sua mensuração no futuro PEREIRA, 2006 P.)

Realizou-se o cálculo da correlação item-total, obtendo os valores apresentados nas tabelas 3, 4 e 5.

TABELA 3

Estatísticas da correlação Item-Total para o agrupamento *Pessoas*

Afirmativas	Média se item for retirado	Variância da Escala se item for retirado	Correlação Item-Total Corrigida	Correlação Múltipla ao Quadrado	Alfa de Cronbach se item for retirado
AFIRMATIVA_3	51,97	0,59	0,02	0,63	0,813
AFIRMATIVA_5	51,90	0,09	0,10	0,43	0,811
AFIRMATIVA_6	52,67	2,78	0,56	0,88	0,794
AFIRMATIVA_7	54,00	8,07	0,16	0,91	0,811
AFIRMATIVA_9	53,40	2,94	0,43	0,81	0,799
AFIRMATIVA_10	54,37	3,07	0,65	0,89	0,792
AFIRMATIVA_15	53,43	1,43	0,43	0,94	0,798
AFIRMATIVA_17	52,50	3,98	0,33	0,92	0,805
AFIRMATIVA_22	53,23	9,08	0,70	0,97	0,784
AFIRMATIVA_24	53,27	0,55	0,49	0,82	0,795
AFIRMATIVA_25	53,30	0,49	0,42	0,90	0,800
AFIRMATIVA_30	53,27	7,17	0,77	0,89	0,779
AFIRMATIVA_35	52,93	1,10	0,60	0,80	0,790
AFIRMATIVA_41	54,53	9,78	0,06	0,84	0,814
AFIRMATIVA_43	51,97	5,21	-0,38	0,87	0,829
AFIRMATIVA_44	53,57	1,98	-0,12	0,80	0,825
AFIRMATIVA_46	53,83	6,21	0,73	0,91	0,779
AFIRMATIVA_47	53,03	0,79	0,55	0,80	0,792
AFIRMATIVA_48	53,97	0,59	0,66	0,79	0,788
AFIRMATIVA_49	52,97	5,14	0,26	0,89	0,808
AFIRMATIVA_50	53,03	0,24	0,58	0,94	0,790
AFIRMATIVA_51	53,27	4,96	-0,29	0,80	0,834

Analisando a tabela percebe-se que as afirmativas que apresentaram correlação positiva item-total menor que 0,5, foram as 3, 5, 7, 9, 15, 17, 24, 25, 41, e 49, haja vista que nesses casos foram atribuídas notas no escalonamento cujos valores apresentam pouca homogeneidade e, com isso, pouca informação para os pesquisadores. Ou seja, esses itens estão prejudicando a fidedignidade do teste.

Já com relação às afirmativas 43, 44 e 51 observa-se correlação negativa, indicando que o item correlaciona-se negativamente com o escore total, ou seja, o comportamento dos respondentes para esse item é o contrário do comportamento do escore total dos respondentes. Destarte, a questão 43 é uma afirmação negativa e de correlação negativa, a maior parte dos respondentes disseram que não concordam e pelos critérios o escore é 3 (discordo parcialmente) e 4 (discordo totalmente). Mas os ítens de avaliação seguem as mesmas diretrizes tendo os mesmos resultados das questões 44 e 45, que auferem pouca homogeneidade e, com isso, pouca informação para os pesquisadores.

Outro valor a ser observado é o valor de alfa de Cronbach se a afirmativa fosse excluída (última coluna da tabela), que mostra o impacto que teria a retirada de cada afirmativa sobre o desempenho do indicador. A retirada da Afirmativa 51 teria o maior impacto positivo sobre o valor do Alfa de Cronbach, que aumentaria de 0,810 para 0,834 (aumento de 3%). Isso mostra que, apesar do valor do item-total, há uma boa consistência interna, já que a retirada de nenhuma variável elevaria de forma expressiva o valor de alfa de Cronbach.

TABELA 4

Estatísticas da correlação Item-Total para o agrupamento Processos

Afirmativas	Média se item for retirado	Variância da Escala se item for retirado	Correlação Item-Total Corrigida	Correlação Múltipla ao Quadrado	Alfa de Cronbach se item for retirado
AFIRMATIVA_8	46,71	3,62	0,37	0,60	0,908
AFIRMATIVA_11	46,60	9,25	0,62	0,70	0,901
AFIRMATIVA_13	46,63	8,71	0,68	0,76	0,899
AFIRMATIVA_14	46,46	1,96	0,46	0,72	0,905
AFIRMATIVA_16	46,77	0,53	0,47	0,76	0,906
AFIRMATIVA_18	46,66	5,06	0,72	0,82	0,897
AFIRMATIVA_19	46,40	8,95	0,63	0,85	0,901
AFIRMATIVA_20	46,40	9,78	0,56	0,79	0,903
AFIRMATIVA_21	45,77	7,65	0,70	0,73	0,898
AFIRMATIVA_23	46,60	8,31	0,65	0,84	0,900
AFIRMATIVA_26	46,74	7,67	0,70	0,80	0,899
AFIRMATIVA_27	46,23	8,12	0,78	0,83	0,897
AFIRMATIVA_28	46,23	6,71	0,74	0,78	0,897
AFIRMATIVA_29	46,60	7,89	0,65	0,71	0,900
AFIRMATIVA_31	46,77	2,65	0,49	0,61	0,905
AFIRMATIVA_37	45,60	8,84	0,06	0,36	0,915
AFIRMATIVA_39	46,06	6,00	0,27	0,48	0,909
AFIRMATIVA_45	45,71	9,03	0,57	0,66	0,903

As afirmativas 8, 14, 16, 31, 37 e 39 apresentam correlação positiva item-total menor que 0,5, fato este que indica que foram atribuídas notas no escalonamento cujos valores apresentam pouca homogeneidade, ou seja, pouca informação para os pesquisadores.

As demais afirmativas demostram boa correlação positiva item-total e, com isso, boa homogeneidade nas respostas, o que indica boa base de informação para o pesquisador.

Outro valor a ser observado é o valor de alfa de Cronbach se a afirmativa fosse excluída (última coluna da tabela), que mostra o impacto que teria a retirada de cada afirmativa sobre o desempenho do indicador. A Afirmativa 37 apresentou o menor valor da correlação item-total, pois apresenta em quase 90% dos casos valores entre 3 e

4 (quase 90% de concordantes). A retirada da Afirmativa 37 elevaria o valor do alfa de Cronbach de 0,907 para 0,915 (0,8%), o que também não seria um aumento expressivo.

TABELA 5

Estatísticas da correlação Item-Total para o agrupamento Tecnologia

Afirmativas	Média se item for retirado	Variância da Escala se item for retirado	Correlação Item-Total Corrigida	Correlação Múltipla ao Quadrado	Alfa de Cronbach se item for retirado
AFIRMATIVA_4	22,48	10,70	0,08	0,39	0,382
AFIRMATIVA_12	23,24	11,31	0,14	0,38	0,346
AFIRMATIVA_32	22,06	8,87	0,45	0,39	0,186
AFIRMATIVA_33	23,55	12,82	-0,16	0,49	0,472
AFIRMATIVA_34	21,97	11,16	0,08	0,30	0,374
AFIRMATIVA_36	21,94	10,31	0,25	0,62	0,298
AFIRMATIVA_38	23,00	11,13	0,07	0,34	0,376
AFIRMATIVA_40	22,00	10,94	0,15	0,56	0,344
AFIRMATIVA_42	21,94	9,75	0,35	0,35	0,249

O agrupamento tecnologias apresentou menor valor de alfa de Cronbach e nenhuma correlação item-total acima de 0,50. Ao analisar esse fator, observa-se que, se a afirmativa 33 fosse excluída, (última coluna da tabela) haveria um aumento de 27% no valor de alfa de Cronbach, ao passo que se a exclusão for da afirmativa 42, o valor do alfa de Cronbach reduziria em 33%.

Esse resultado pode sugerir dificuldade na interpretação das afirmativas, ou que um novo agrupamento pode gerar melhores resultados.

5.3.3 – Capacidade de Generalização

O último ítem do processo de validação do instrumento de coleta de dados é a capacidade de generalização. Conforme dito na metodologia, Malhotra (2012, p.232) adverte que “a capacidade de generalização é uma indicação de até que ponto um estudo baseado em uma amostra se aplica a um universo de generalizações”.

O desenvolvimento da capacidade de generalização do instrumento de coleta de dados será feito por agrupamento – pessoas, processos e tecnologias. Segue-se esse formato para esse caso porque os cálculos têm como prerrogativa o agrupamento das

variáveis. Esta sessão terá inicio com os estudos de capacidade de generalização do agrupamento pessoas.

Segundo Hair (2009, p.106), “se o pesquisador incluir indiscriminadamente um grande número de variáveis e esperar que a análise fatorial “arrume as coisas”, então torna-se elevada a possibilidade de resultados pobres”. Dessa forma, considerando que a análise fatorial considera a correlação entre as variáveis, foram retiradas as variáveis que não apresentaram correlação positiva acima de 30% com pelo menos duas variáveis.

Nesse primeiro momento, foram excluídas as variáveis que compõem as afirmativas: Q3, Q5, Q43, Q44, Q51, Q17, Q41 e Q49. É importante observar, também, que todas as variáveis excluídas apresentaram correlação item-total menores que 0,5 (Tabela X), sendo a única exceção a afirmativa 7, que embora tenha apresentado correlação item-total menor que 0,5, tem correlação significativa, acima de 30%, com 3 variáveis.

Os resultados obtidos com a análise fatorial devem ser analisados com cautela, uma vez que várias suposições da aplicação da análise fatorial, conforme Hair (2009), não são atendidas, tais como: amostra com tamanho inferior a 50 respondentes, as variáveis não seguem distribuição normal, proporção menor que 5 para 1 (5 respostas para cada variável), e maior parte da amostra não apresenta correlação acima de 30%.

O método utilizado para a análise fatorial foi a rotação Varimax (MALHOTRA, 2012; HAIR (2009). A rotação Varimax, conforme Pestana **&** Gageiro (1998) é uma rotação ortogonal, que minimiza o número de variáveis com elevados *loadings* (valor do coeficiente de correlação entre a variável e o fator obtido) num fator. Em geral, são considerados significativos *loadings* iguais ou superiores a 0,5. Os valores faltantes foram substituídos pelo valor médio de cada variável.

O teste de esfericidade de Bartlett pode ser utilizado para testar a hipótese de que a matriz das correlações seja a matriz identidade. Como o valor encontrado foi menor que o nível de significância (<0,001), levando à rejeição da hipótese nula, ou seja, existe correlação entre as variáveis. O teste de Kaiser-Meyer_Olkin (KMO) compara as correlações simples com as parciais observadas entre as variáveis. Valor de KMO perto de 1 indica coeficiente de correlação parciais pequenos, enquanto valores próximos de zero indica que a análise fatorial pode não ser adequada, pois as correlações existentes entre as variáveis são fracas. Considerando o valore observado do teste, KMO=0,705,

conclui-se que a análise fatorial é mediana, permitindo o prosseguimento da análise fatorial.

A análise da matriz anti-imagem não mostrou nenhum valor da linha diagonal inferior a 0,5.

Utilizando o critério de Kaiser e o Scree Plot, extraiu-se 4 fatores que explicam 70,2% da variância da amostra.

Os valores das comunalidades representam a proporção da variância para cada variável incluída na análise que é explicada pelos componentes extraídos. Usualmente, o valor aceitável é de 0,50. Para os valores abaixo de 0,5, as variáveis devem ser excluídas e a análise fatorial realizada novamente. Exclui-se a variável Q6, que apresentava valor abaixo de 0,5 (0,462).

Executando-se novamente a análise fatorial, obteve-se KMO=0,760, p-valor do teste de esfericidade de Bartellet <0,001. Não houve nenhuma comunalidade abaixo de 0,5 e a matriz anti-imagem não apresentou nenhum valor na diagonal principal inferior a 0,5.

Deve-se analisar também as cargas fatoriais de cada variável em relação aos componentes extraídos. Observando-se a matriz rotacionada, deve-se identificar as variáveis que apresentam elevadas cargas fatoriais para mais de um fator, no caso valores acima de 0,4. Essas variáveis devem ser retiradas, pois elas contribuem para a construção de fatores distintos. Hair (2009) afirma que, nesse caso, entre outros métodos, pode-se ignorar as variáveis problemáticas e interpretar a solução como ela é, ou avaliar cada uma das variáveis para possível eliminação. Optou-se por excluir as variáveis que apresentaram elevadas cargas fatoriais para mais de um fator, eliminando-se assim as variáveis Q47, Q9, Q24,Q15, Q50, Q25.

Após a execução de nova análise fatorial, obteve KMO=0,668, p-valor do teste de esfericidade de Bartellet <0,001. E dois fatores explicando 62,6% da variância. Como a matriz anti-imagem apresentou valor inferior a 0,5 para a variável Q7, optou-se por eliminá-la.

Após nova execução da análise fatorial, obteve-se KMO=0,686, p-valor do teste de esfericidade de Bartellet <0,001. Nenhuma variável apresentou comunalidade abaixo de 0,50, da mesma forma, a matriz anti-imagem não apresentou valor na diagonal menor que 0,5, nem cargas fatoriais acima de 0,4 para mais de um fator. Obtendo-se apenas um fator explicando 53,7% da variância.

TABELA 6

Afirmativas com maiores valores de variâncias

Variáveis	Componente 1
Afirmativa_6	,574
Afirmativa_10	,781
Afirmativa_22	,742
Afirmativa_30	,785
Afirmativa_35	,635
Afirmativa_46	,819
Afirmativa_48	,760

Ao final da análise fatorial, obteve-se um fator, com 7 variáveis, que explica 53,7% da variância total. Dessa forma, para as 7 variáveis em questão, a dimensionalidade é igual a 1.

De mesmo modo realizou-se a análise fatorial para o agrupamento processos e tecnologias.

No agrupamento processos, retirou-se as variáveis Q37, pois não apresentou correlação positiva acima de 30% com nenhuma variável. O valor do teste KMO=0,748 e teste de esfericidade de Bartellet <0,001. Nenhuma variável apresentou comunalidade abaixo de 0,50, da mesma forma, a matriz anti-imagem não apresentou valor na diagonal menor que 0,5. Obteve-se 4 fatores, que conjuntamente explicam 71,3% da variância.

Como devem ser analisadas, também, as cargas fatoriais de cada variável em relação aos componentes extraídos, observando-se a matriz rotacionada, identificou-se as variáveis que apresentam elevadas cargas fatoriais para mais de um fator, no caso valores acima de 0,4, que foram retiradas: Q11, Q18, Q19, Q20,Q23, Q26 e Q45.

Após nova execução da análise fatorial, obteve-se do teste KMO=0,765 e teste de esfericidade de Bartellet <0,001. A matriz anti-imagem não apresentou valor na diagonal menor que 0,5, porém a variável Q39 apresentou comunalidade abaixo de 0,50.

Continuou-se realizando todos os procedimentos já descritos até chegar na análise fatorial com teste de KMO=0,789, teste de esfericidade de Bartellet <0,001. Tanto a diagonal principal da matriz anti-imagem como as comunalidades apresentaram

valores maior que 0,5. Obtiveram-se três fatores, com 8 variáveis, que explicam 75,6% da variância total.

O primeiro fator, que explica 40,5% da variância, está relacionado as variáveis Q29,Q28, Q21, Q27 e Q31, o segundo fator, que explica 21,4% da variável está relacionado às variáveis Q8 e Q14, e o terceiro fator que explica 13,7% da variância, está relacionado à variável Q39.

TABELA 7

Relação de variáveis e Escala de variâncias

Variáveis	Componentes		
	1	2	3
Afirmativa_29	,814	-,041	,315
Afirmativa_28	,808	,280	,008
Afirmativa_21	,807	,340	-,101
Afirmativa_27	,804	,295	,135
Afirmativa_31	,755	-,170	,013
Afirmativa_8	,021	,860	-,026
Afirmativa_14	,210	,809	,141
Afirmativa_39	,089	,082	,972

Ao realizar a análise fatorial para o agrupamento tecnologias, obteve-se o valor de KMO=0,467, indicando que a análise fatorial não é a melhor forma de análise para esse grupo. Esse resultado já era esperado, como observado na tabela Z, não houve nenhuma correlação item-total acima de 0,5. Das 9 variáveis nesse grupo, 7 se correlacionam com apenas 1 variável.

Considerando apenas as variáveis Q32, Q36 e Q40, que apresentaram correlações positivas, obteve-se KMO=0,581, mas o valor do teste de Bartellet =0,055 indicou pouca correlação entre as variáveis, o que novamente contra indica o uso da análise fatorial.

Nesse tipo de aplicação, a análise fatorial tinha como principal objetivo comprovar a unidimensionalidade do instrumento de coleta para cada agrupamento. O reduzido tamanho da amostra comprometeu a análise capacidade de generalização do instrumento de coleta de dados. Para que os dados tivessem uma capacidade de generalização expressiva havia necessidade que os números de respostas (35) fossem

maior que o número de perguntas (51). Mesmo diante desse fato os cálculos e análises foram feitos.

A partir das análises pode-se perceber que as afirmativas negativas, em sua maioria, não se correlacionam positivamente de forma significativa, indicando que pode ter havido dificuldade na sua interpretação.

5.4 – Análise descritiva dos dados

Iniciando a análise dos dados primários, inicialmente pode-se perceber, com relação ao perfil dos 35 respondentes, que 49% (17) são mulheres e 51% (18) homens. Em relação à escolaridade, 6% (2) possuem o 2º grau completo e 94% (33) ensino superior completo.

TABELA 8

Distribuição por sexo e escolaridade

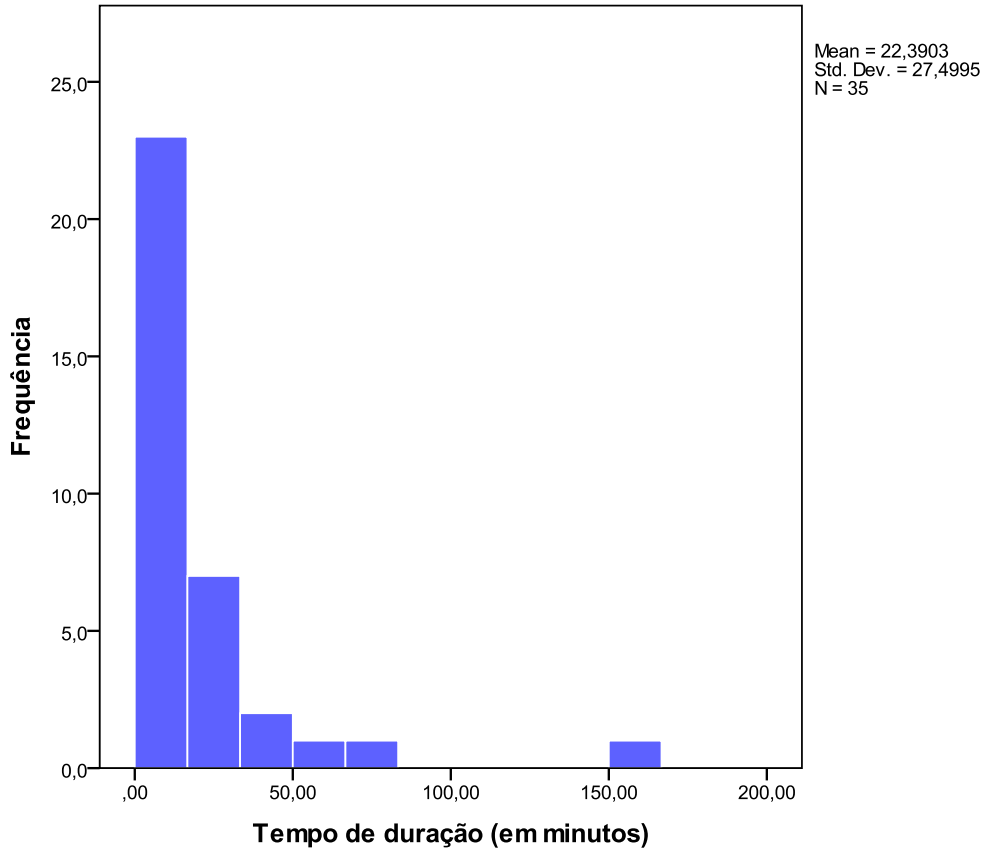
Escolaridade	Sexo		Total
	Feminino	Masculino	
Segundo grau completo	1	1	2
Superior completo	16	17	33
Total	17	18	35

O tempo mínimo de resposta do questionário foi de 6,5 minutos e máximo de 2 horas e 7 minutos. O tempo médio foi de 22,4 minutos e desvio-padrão de 27,5. Retirando os três valores considerados extremos, o valor mínimo se manteve, o tempo máximo reduziu para 37,9 minutos, média de 15,6 e desvio-padrão de 8,3 minutos (Gráfico 1).

Considerando que o questionário possuía ao todo 51 questões, o tempo médio de resposta para cada questão foi de 18,3 segundos.

GRÁFICO 1

Tempo em minutos de resposta do questionário



Observa-se que nem todos os colaboradores que participaram da pesquisa responderam a todas as questões, gerando uma análise de dados ausentes.

Infelizmente o site kiwiksurveys.com não possui mecanismo de parar o prosseguimento das respostas caso o respondente deixe uma resposta em branco. Nesse sentido para o agrupamento “Pessoas”, o percentual de dados ausentes foi de 0,8% (apenas 6 não respostas e 764 respostas válidas). No agrupamento “Processos” não houve dados ausentes, e no agrupamento “Tecnologias” o percentual de dados ausentes foi de 1%. No total, o percentual de dados ausentes foi de 0,5%.

Já com relação à análise da normalidade, conforme dito na seção de metodologia, foi utilizado o teste de Normalidade Shapiro-Wilk, recomendado para amostras cuja dimensão é 50, com o objetivo de testar se as variáveis seguem uma distribuição normal.

Com os resultados obtidos pelo p-valor, pode-se concluir que, a 5% de significância, nenhuma variável segue uma distribuição normal. Seguem tabelas:

TABELA 9

Teste de Normalidade para as variáveis do agrupamento “Pessoas”

Teste de Normalidade - Shapiro- Wilk			
Afirmativas	Estatística	Graus de liberdade	P-valor
Afirmativa_3	0,491	35	<0,001
Afirmativa_5	0,458	35	<0,001
Afirmativa_6	0,779	35	<0,001
Afirmativa_7	0,817	35	<0,001
Afirmativa_9	0,837	34	<0,001
Afirmativa_10	0,612	35	<0,001
Afirmativa_15	0,859	35	<0,001
Afirmativa_17	0,721	35	<0,001
Afirmativa_22	0,871	35	0,001
Afirmativa_24	0,866	35	0,001
Afirmativa_25	0,818	35	<0,001
Afirmativa_30	0,884	35	0,001
Afirmativa_35	0,764	33	<0,001
Afirmativa_41	0,376	34	<0,001
Afirmativa_43	0,477	34	<0,001
Afirmativa_44	0,868	35	0,001
Afirmativa_46	0,789	35	<0,001
Afirmativa_47	0,871	35	0,001
Afirmativa_48	0,804	35	<0,001
Afirmativa_49	0,852	35	<0,001
Afirmativa_50	0,863	34	0,001
Afirmativa_51	0,871	35	0,001

TABELA 10

Teste de Normalidade para as variáveis do agrupamento “Processos”

Teste de Normalidade - Shapiro- Wilk			
	Estatística	Graus de liberdade	P-valor
Afirmativa_8	0,874	35	0,001
Afirmativa_11	0,878	35	0,001
Afirmativa_13	0,862	35	<0,0001
Afirmativa_14	0,856	35	<0,0001
Afirmativa_16	0,878	35	0,001
Afirmativa_18	0,862	35	<0,0001
Afirmativa_19	0,859	35	<0,0001
Afirmativa_20	0,843	35	<0,0001
Afirmativa_21	0,718	35	<0,0001
Afirmativa_23	0,883	35	0,001
Afirmativa_26	0,880	35	0,001
Afirmativa_27	0,854	35	<0,0001
Afirmativa_28	0,855	35	<0,0001
Afirmativa_29	0,856	35	<0,0001
Afirmativa_31	0,854	35	<0,0001
Afirmativa_37	0,667	35	<0,0001
Afirmativa_39	0,810	35	<0,0001
Afirmativa_45	0,648	35	<0,0001

TABELA 11

Teste de Normalidade para as variáveis do agrupamento “Tecnologias”

Teste de Normalidade - Shapiro- Wilk			
	Estatística	Graus de liberdade	P-valor
Afirmativa_4	0,821	35	<0,001
Afirmativa_12	0,806	35	<0,001
Afirmativa_32	0,767	35	<0,001
Afirmativa_33	0,745	34	<0,001
Afirmativa_34	0,710	34	<0,001
Afirmativa_36	0,729	35	<0,001
Afirmativa_38	0,858	35	<0,001
Afirmativa_40	0,748	34	<0,001
Afirmativa_42	0,739	35	<0,001

Feito o teste de normalidade, prossegue-se com a correlação das variáveis. Como os dados não seguem uma distribuição normal, utilizou-se o coeficiente de correlação de Spearman. O coeficiente de correlação de Spearman utiliza os valores das observações em vez do valor observado, não sendo, portanto, sensível a assimetrias na distribuição, nem à presença de *outliers.*

O agrupamento "Pessoas" apresentou 49% das correlações significativas, ou seja, das 231 correlações 2 a 2 (22*21/2), para 114, o p-valor encontrado foi menor que 5%, indicando correlação significativa. No agrupamento "Processos" 52,3 % das correlações foram significativas e no agrupamento "Tecnologias" o percentual de correlações significativas foi de 11%.

Para entender o posicionamento dos recursos humanos da organização sob o aspecto da segurança da informação, inicia-se a análise descritiva buscando entender qual a informação está descrita através da codificação dos números obtidos na coleta de dados (PASQUALI, 2001). Ressalta-se que a análise dos percentuais e o cruzamento entre as variáveis ocorrerá na seção de discussão dos resultados. Conforme descrito na metodologia, optou-se por dividir esses dados em agrupamentos seguindo os três pilares da gestão de segurança informacional: *pessoas*, *processos* e *tecnologias*.

O primeiro agrupamento a ser discutido é *pessoas*.

Com base nos dados disponibilizados na tabela a seguir, na qual se tem a distribuição de participantes discordantes e concordantes e seu detalhamento com relação às questões do grupo pessoas, observa-se:

TABELA 12

	Discordantes		Concordantes		NR		Total	
Variáveis	N	%	N	%	N	%	N	%
Afirmativa_3			35	100			35	100
Afirmativa_5			35	100			35	100
Afirmativa_6	5	14,3	30	85,7			35	100
Afirmativa_7*	28	80	7	20			35	100
Afirmativa_9	17	48,6	17	48,6	1	2,9	35	100
Afirmativa_10	25	71,4	10	28,6			35	100
Afirmativa_15	20	57,1	15	42,9			35	100
Afirmativa_17	6	17,1	29	82,9			35	100
Afirmativa_22	16	45,7	19	54,3			35	100
Afirmativa_24	17	48,6	18	51,4			35	100
Afirmativa_25	15	42,9	20	57,1			35	100
Afirmativa_30	18	51,4	17	48,6			35	100
Afirmativa_35	7	20	26	74,3	2	5,7	35	100
Afirmativa_41	31	88,6	3	8,6	1	2,9	35	100
Afirmativa_43*	3	8,6	31	88,6	1	2,9	35	100
Afirmativa_44	23	65,7	12	34,3			35	100
Afirmativa_46	23	65,7	12	34,3			35	100
Afirmativa_47	16	45,7	19	54,3			35	100
Afirmativa_48	27	77,1	8	22,9			35	100
Afirmativa_49	11	31,4	24	68,6			35	100
Afirmativa_50	12	34,3	22	62,9	1	2,9	35	100
Afirmativa_51	15	42,9	20	57,1			35	100

Distribuição dos participantes discordantes e concordantes das afirmativas do agrupamento “Pessoas”

Para o agrupamento “Pessoas” a média geral, de acordo com as médias observadas para cada afirmativa, foi de 2,5.

As questões nas quais houve 80% ou mais de concordância foram as de número 6, 17 e 43. Comparativamente, as questões com maior número de discordantes são 7, 10, 41 e 48.

Na sequência da análise, observa-se que a afirmativa com o maior percentual de não respostas foi a 35, com 6% de não respostas. Curiosamente, essa questão pergunta aos colaboradores se há envolvimento e apoio das gerências, diretorias e presidência, no que concerne às ações de segurança da informação praticada na instituição.

Abaixo segue a tabela da análise descritiva dos dados com base na escala da Likert.

TABELA 13

Número de concordantes e discordantes das afirmativas do agrupamento "Pessoas"

Afirmativas	Discordo Totalmente	Discordo Parcialmente	Concordo Parcialmente	Concordo Totalmente	NR	Total	Média	Mediana	Desvio-Padrão	Soma
	1	2	3	4						
Afirmativa_3			20%	80%		100%	3,8	4	0,41	133
Afirmativa_5			17%	83%		100%	3,8	4	0,38	134
Afirmativa_6	6%	9%	60%	26%		100%	3,1	3	0,77	107
Afirmativa_7*	40%	40%	14%	6%		100%	1,9	2	0,88	65
Afirmativa_9	26%	23%	43%	6%	3%	100%	2,3	3	0,94	78
Afirmativa_10	71%	20%	9%			100%	1,4	1	0,65	48
Afirmativa_15	31%	26%	29%	14%		100%	2,3	2	1,07	79
Afirmativa_17	14%	3%	31%	51%		100%	3,2	4	1,05	112
Afirmativa_22	17%	29%	43%	11%		100%	2,5	3	0,92	87
Afirmativa_24	26%	23%	34%	17%		100%	2,4	3	1,07	85
Afirmativa_25	31%	11%	29%	29%		100%	2,5	3	1,22	89
Afirmativa_30	17%	34%	34%	14%		100%	2,5	2	0,95	86
Afirmativa_35	11%	9%	60%	14%	6%	100%	2,8	3	0,85	93
Afirmativa_41	86%	3%	3%	6%	3%	100%	1,3	1	0,79	43
Afirmativa_43*	3%	6%	9%	80%	3%	100%	3,7	4	0,72	126
Afirmativa_44	23%	43%	29%	6%		100%	2,2	2	0,86	79
Afirmativa_46	49%	17%	23%	11%		100%	2	2	1,1	69
Afirmativa_47	11%	34%	29%	26%		100%	2,7	3	0,99	94
Afirmativa_48	46%	31%	17%	6%		100%	1,8	2	0,92	64
Afirmativa_49	14%	17%	43%	26%		100%	2,8	3	0,99	98
Afirmativa_50	14%	20%	43%	20%	3%	100%	2,7	3	0,97	92
Afirmativa_51	17%	26%	43%	14%		100%	2,5	3	0,95	89

*Afirmativas com lógica inversa

Através dessa tabela, demonstra-se o percentual de concordância e discordância para cada afirmativa que compõe a arena pessoas.

Considerando que a escala varia de 1 a 4, e quanto maior o valor atribuído, maior a concordância dos respondentes com a afirmativa apresentada, as afirmativas que apresentaram maiores médias foram 5, 3, 43, 17, 6 e 49. Ou seja, houve um maior número de respondentes que concordaram com essas afirmativas, e as afirmativas em que houve maior número de discordância, e consequentemente apresentaram menor média foram 22, 21, 20, 19 e 18. Obtém-se interpretação semelhante analisando o valor da soma total para cada item.

Os dados exibidos na tabela referentes à média trazem informação que as questões 3, 5, 6, 17 e 43, por terem valores mais próximos a 4, indicam que os respondentes concordaram mais com essas respostas. Paralelamente, as questões 7, 10, 41 e 48 obtiveram valores mais distantes de 4, indicando que os respondentes discordaram mais nessas afirmativas.

Os dados do desvio padrão trazem informações sobre o quanto os valores, em média, variaram em torno da média, as afirmativas que apresentaram maior desvio-padrão foram as de número 15, 24, 25 e 46, indicando que se trata de afirmativas onde houve maior dispersão nas respostas.

Para as 22 afirmativas avaliadas, a média do escore total foi de 88,6. Com desvio-padrão de 23,96.

O segundo agrupamento a ser discutido é *processos*.

TABELA 14

	Discordantes		Concordantes		NR		Total	
Variáveis	N	%	N	%	N	%	N	%
Afirmativa_8	19	54,3	16	45,7			35	100
Afirmativa _11	18	51,4	17	48,6			35	100
Afirmativa _13	16	45,7	19	54,3			35	100
Afirmativa _14	17	48,6	18	51,4			35	100
Afirmativa _16	20	57,1	15	42,9			35	100
Afirmativa _18	20	57,1	15	42,9			35	100
Afirmativa _19	16	45,7	19	54,3			35	100
Afirmativa _20	17	48,6	18	51,4			35	100
Afirmativa _21	8	22,9	27	77,1			35	100
Afirmativa _23	17	48,6	18	51,4			35	100
Afirmativa _26	20	57,1	15	42,9			35	100
Afirmativa _27	11	31,4	24	68,6			35	100
Afirmativa _28	13	37,1	22	62,9			35	100
Afirmativa _29	20	57,1	15	42,9			35	100
Afirmativa _31	21	46,7	24	53,3			45	100
Afirmativa _37*	4	11,4	31	88,6			35	100
Afirmativa _39	8	22,9	27	77,1			35	100
Afirmativa _45	8	22,9	27	77,1			35	100

Distribuição dos participantes discordantes e concordantes das afirmativas do agrupamento “Processos”

Para o agrupamento “Processos” a média das médias observadas para cada afirmativa foi de 2,7, média maior que do agrupamento pessoas.

As questões nas quais houve 70% ou mais de concordância foram as de número 21, 37, 39 e 45. Comparativamente, as questões com maior número de discordantes são 16, 18, 26 e 29.

Não ocorreram não respostas no agrupamento *processos*.

TABELA 15

Número de concordantes e discordantes das afirmativas do agrupamento "Processos"

	Discordo 1	Discordo 2	Concordo 3	Concordo 4	NR	Total	Média	Mediana	Desvio-Padrão	Soma
Afirmativa_8	14%	40%	37%	9%		100%	2,4	2	0,85	84
Afirmativa_11	11%	40%	34%	14%		100%	2,51	2	0,89	88
Afirmativa_13	14%	31%	46%	9%		100%	2,49	3	0,85	87
Afirmativa_14	6%	43%	31%	20%		100%	2,66	3	0,87	93
Afirmativa_16	23%	34%	29%	14%		100%	2,34	2	1	82
Afirmativa_18	20%	37%	20%	23%		100%	2,46	2	1,07	86
Afirmativa_19	6%	40%	31%	23%		100%	2,71	3	0,89	95
Afirmativa_20	6%	43%	26%	26%		100%	2,71	3	0,83	95
Afirmativa_21	3%	20%	17%	60%		100%	3,34	4	0,91	117
Afirmativa_23	14%	34%	37%	14%		100%	2,51	3	0,92	88
Afirmativa_26	17%	40%	31%	11%		100%	2,37	2	0,91	83
Afirmativa_27	3%	29%	46%	23%		100%	2,89	3	0,8	101
Afirmativa_28	6%	31%	31%	31%		100%	2,89	3	0,93	101
Afirmativa_29	11%	46%	23%	20%		100%	2,51	2	0,95	88
Afirmativa_31	11%	49%	34%	6%		100%	2,34	2	0,77	82
Afirmativa_37	3%	9%	23%	66%		100%	3,51	4	0,78	123
Afirmativa_39		23%	49%	29%		100%	3,06	3	0,73	107
Afirmativa_45	6%	17%	9%	69%		100%	3,4	4	0,98	119

*Afirmativas com lógica inversa

Através dessa tabela demonstra-se o percentual de concordância e discordância para cada afirmativa que compõe a arena processos.

Considerando que a escala varia de 1 a 4, e quanto maior o valor atribuído, maior a concordância dos respondentes com a afirmativa apresentada, as afirmativas que apresentaram maiores médias foram 21, 37, 39 e 45. Ou seja, houve um maior número de respondentes que concordaram com essas afirmativas, e as afirmativas em que houve maior número de discordância, e consequentemente apresentaram as menores médias, foram 8, 13, 16, 18, 26 e 31. Obtém-se interpretação semelhante analisando o valor da soma total para cada item.

Os dados exibidos na tabela referentes à média trazem informação que as questões 21, 37, 39 e 45, por terem valores mais próximos a 4, indicam que os respondentes concordaram mais com essas respostas. Paralelamente, as questões 8, 13, 16, 18, 26 e 31 obtiveram valores mais distantes de 4, indicando que os respondentes discordaram mais nessas afirmativas.

Os dados do desvio padrão trazem informações sobre o quanto os valores, em média, variaram em torno da média, as afirmativas que apresentaram maior desvio-

padrão foram as de número 16 e 18, indicando que se trata de afirmativas onde houve maior dispersão nas respostas.

O último agrupamento a ser discutido é o de tecnologia.

Os dados disponibilizados na tabela a seguir demonstram a distribuição de participantes discordantes e concordantes e seu detalhamento com relação às questões do grupo tecnologia.

TABELA 16

Distribuição dos participantes discordantes e concordantes das afirmativas do agrupamento "Tecnologia"

	Discordantes		Concordantes		NR		Total	
Variáveis	N	%	N	%	N	%	N	%
Afirmativa_4*	15	42,9	20	57,1			35	100
Afirmativa_12	28	80	7	20			35	100
Afirmativa_32	9	25,7	26	74,3			35	100
Afirmativa_33	28	80	6	17,1	1	2,9	35	100
Afirmativa_34*	6	17,1	28	80	1	2,9	35	100
Afirmativa_36*	7	20	28	80			35	100
Afirmativa_38	23	65,7	12	34,3			35	100
Afirmativa_40	8	22,9	26	74,3	1	2,9	35	100
Afirmativa_42	8	22,9	27	77,1			35	100

Para o agrupamento "Tecnologia" a média geral observada para cada afirmativa foi de 2,8.

As questões nas quais houve 70% ou mais de concordância foram as de número 32, 40 e 42. Comparativamente, as questões com maior número de discordantes são as de número 4 e 38.

Na sequência da análise, observa-se que as afirmativas com o maior percentual de não respostas foram as questões 33, 34 e 40, com 1% de não respostas para cada uma.

A seguir tabela da análise descritiva dos dados, com base na escala da Likert.

TABELA 17

Número de concordantes e discordantes das afirmativas do agrupamento "Tecnologia"

	Totalmente 1	Parcialmente 2	Totalmente 3	Totalmente 4	NR	Total	Média	Mediana	Desvio-Padrão	Soma
Afirmativa_4*	17%	26%	17%	40%		100%	2,8	3	1,16	98
Afirmativa_12	20%	60%	14%	6%		100%	2,1	2	0,76	72
Afirmativa_32	11%	14%	23%	51%		100%	3,1	4	1,06	110
Afirmativa_33	51%	29%	9%	9%	3%	100%	1,7	1	0,96	59
Afirmativa_34*	9%	9%	23%	57%	3%	100%	3,3	4	0,98	113
Afirmativa_36*	9%	11%	23%	57%		100%	3,3	4	0,99	115
Afirmativa_38	29%	37%	20%	14%		100%	2,2	2	1,02	77
Afirmativa_40	3%	20%	20%	54%	3%	100%	3,3	4	0,91	112
Afirmativa_42	3%	20%	20%	57%		100%	3,3	4	0,9	116

*Afirmativas com lógica inversa

Através dessa tabela, demonstra-se o percentual de concordância e discordância para cada afirmativa que compõe a arena *processos*.

Considerando que a escala varia de 1 a 4, e quanto maior o valor atribuído, maior a concordância dos respondentes com a afirmativa apresentada, as afirmativas que apresentaram maiores médias foram 32, 34, 36, 40 e 42. Ou seja, houve um maior número de respondentes que concordaram com essas afirmativas, e a afirmativa em que houve maior número de discordância e, consequentemente, apresenta menor média foi a questão 33. Obtém-se interpretação semelhante analisando o valor da soma total para cada item.

Os dados exibidos na tabela referentes à média trazem informação de que as questões 32, 34, 36, 40 e 42, por terem valores mais próximos a quatro, indicam que os respondentes concordaram mais com essas respostas. Paralelamente, a questão 33 obteve o valor mais distante de 4, indicando que os respondentes discordaram mais nessa afirmativa.

Os dados do desvio padrão trazem informações sobre o quanto os valores variaram em torno da média. As afirmativas que apresentaram maior desvio-padrão foram as de número 04, 32 e 38, indicando que se trata de afirmativas onde houve maior dispersão nas respostas.

Através da tabela final abaixo expressa, observa-se que a maior média está localizada no agrupamento *tecnologias*. Isso indica que os respondentes concordaram mais com essas respostas. Os dados do desvio padrão trazem informações sobre o quanto os valores variaram em torno da média, as afirmativas que apresentaram maior

desvio-padrão foram as do agrupamento *pessoas*, indicando que se trata de afirmativas onde houve maior dispersão nas respostas.

TABELA 18

Estatísticas descritivas da soma dos escores por agrupamentos

	N	Mínimo	Máximo	Média	Desvio-Padrão	CV
Pessoas	22	43	134	88,6	23,96	27,0%
Processos	18	82	123	95,5	13,18	13,8%
Tecnologias	9	59	116	96,9	21,81	22,5%

6 - Discussão dos resultados

Nessa fase de discussão dos resultados propõem-se cruzar as respostas das perguntas e fazer análises. Essa etapa é importante no sentido de que as perguntas podem ser interpretadas em mais de uma arena, e, dessa forma o pesquisador ficaria livre para fazer outras considerações sem se prender ao agrupamento das questões em arenas, conforme previamente apresentado. Essa ação visa o enriquecimento do estudo buscando outros pontos de análise e, consequentemente, um conjunto mais solidificado de informações que são base para a composição dos cenários de gestão de segurança informacional na instituição pesquisada.

Através da discussão dos resultados auferidos pretende-se apresentar percepções no que concerne à leitura dos pesquisadores com relação às respostas obtidas sobre a temática segurança da informação e os cenários encontrados na instituição pesquisada. Esse cenários estão subdivididos em : Cenário de aspectos gerais sobre segurança da informação; Cenário de comportamental dos colaboradores; Cenário de déficit comunicacional e, por último, cenário de informações relativas à tecnologia.

6.1 - Cenário de aspectos gerais sobre segurança da informação

Logo no início do questionário foram indagadas questões relativas ao entendimento do colaborador sobre o significado de segurança da informação e, na sequência, seu sentimento como forma de se reconhecer como parte responsável pela segurança da informação na instituição pesquisada. Para ambas as afirmativas, números 3 e 5, 100% dos respondentes foram concordantes. Dessa forma, quantitativamente, essas afirmativas apresentam maiores médias: 3,8, maior soma (peso) na escala de Likert e, paralelamente, menores coeficientes de variação, haja vista que, conforme informado anteriormente, quanto maior a variação menor será a quantidade de informações que poderão ser extraídas pelos pesquisadores de cada questão.

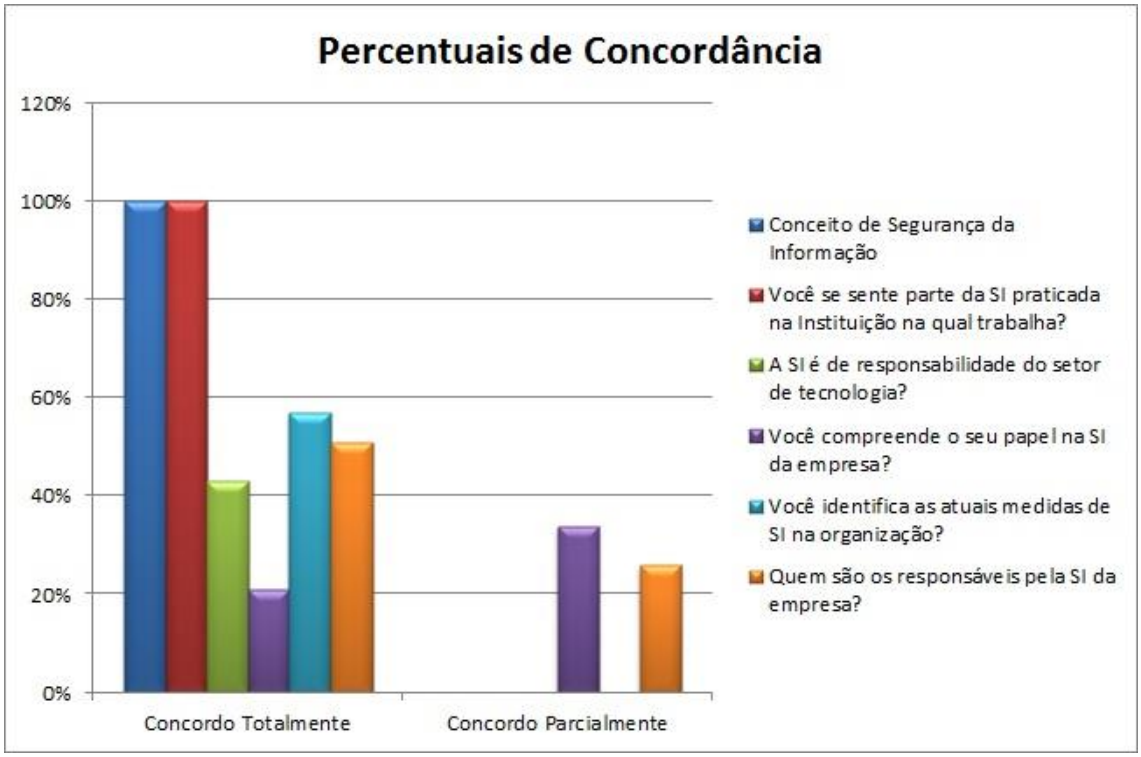
Destarte, a discrepância começa a aparecer quando os colaboradores são questionados sobre suas capacidades de identificar as atuais medidas que estão sendo tomadas em relação à segurança da informação na instituição (questão 23), 57%

afirmam que conseguem identificar essas medidas e 43% afirmam que não conseguem identificar essas medidas. Como entender o que é segurança da informação e se sentir parte dela sem haver uma maioria expressiva que compreende as ações que estão sendo desenvolvidas pela empresa como corroborativas à gestão de segurança informacional nesta?

Buscando entender com clareza como os colaboradores compreendem seu papel na segurança informacional da empresa (questão 47), os novos dados obtidos indicam que pouco mais da metade dos respondentes (55%) concordam que sabem com clareza qual é o seu papel, embora 34% deste total concordam parcialmente com a afirmativa, ou seja, em mais da metade dos concordantes ainda há dúvidas.

Doravante, quando questionados sobre os responsáveis pela segurança informacional da empresa, 77% sabem quem são essas pessoas, sendo que 51% sabem com total certeza (concordo totalmente). Complementar a essa reflexão, observa-se que 43% dos respondentes concordam que a segurança da informação é responsabilidade do setor de tecnologia da informação e 57% discordam da afirmativa.

GRAFICO 2:



Nota-se que um número muito alto de pessoas acredita na abordagem técnica às questões de segurança da informação e talvez seja esse um dos motivos pelos

quais os colaboradores não consigam identificar com clareza seu papel na segurança informacional da organização. Apesar de saberem com lucidez que são os responsáveis pela segurança informacional corporativa, eles não conhecem com a mesma transparência as atuais medidas em vigor na instituição no que concerne à segurança da informação.

Um cenário com fortes veios firmados na abordagem tecnológica não poderia ter outro resultado, pessoas se estruturando totalmente nas tecnologias e fazendo delas a solução cômoda para todos os problemas de insegurança informacional.

A questão 35 propõe reflexão complementar à perspectiva apresentada acima, uma vez que 74% dos respondentes ratificam que há envolvimento e apoio das gerências, diretorias e presidência com relação às ações de segurança da informação. O total de 60% das respostas se concentrou na esfera de "concordo parcialmente" com a afirmativa. Logicamente, por se tratar de uma afirmativa parcial, não se pode deixar de ressalvar que talvez o envolvimento do *staff* da empresa ainda esteja a desejar na perspectiva dos funcionários. Paralelamente, umas das interpretações que esses dados trazem é que existem pessoas responsáveis pela segurança da informação de modo que o usuário não precise se envolver, ou que existem equipes ou comitês bem formados e que se posicionam frente à questão da segurança da informação de forma muito proativa juntos aos funcionários.

Quando a pergunta no questionário se refere aos critérios de classificação da informação para garantir a confidencialidade, integridade e disponibilidade dos ativos informacionais da instituição, ou seja, uma das formas de se garantir a segurança da informação corporativa, mais de 80% dos entrevistados concordaram demonstrando uma aceitação expressiva daqueles que afirmaram que conseguem agir seguramente. Destarte, quando se desmembra o total apresentado de 80% de concordância, observa-se que 60% dos respondentes concordam parcialmente com a afirmativa, demonstrando que ainda podem existir dúvidas com relação aos critérios de classificação das informações visando a segurança da informação.

Nessa mesma linha há um questionamento para entender a perspectiva do leitor no que concerne às políticas de informação e os critérios de classificação da informação mencionados acima. Os respondentes entendem que as políticas de informação da organização são um veículo eficiente e efetivo para garantir a confidencialidade, integridade e disponibilidade das informações corporativas,

entretanto essa percepção é parcial, haja vista que 46% dos respondentes concordam parcialmente e 34% discordam parcialmente, demonstrando que são necessárias ações para que haja uma convergência efetiva entre as necessidades dos recursos humanos e a forma de posicionamento, organização para controle, comunicação e expressão das políticas informacionais da organização.

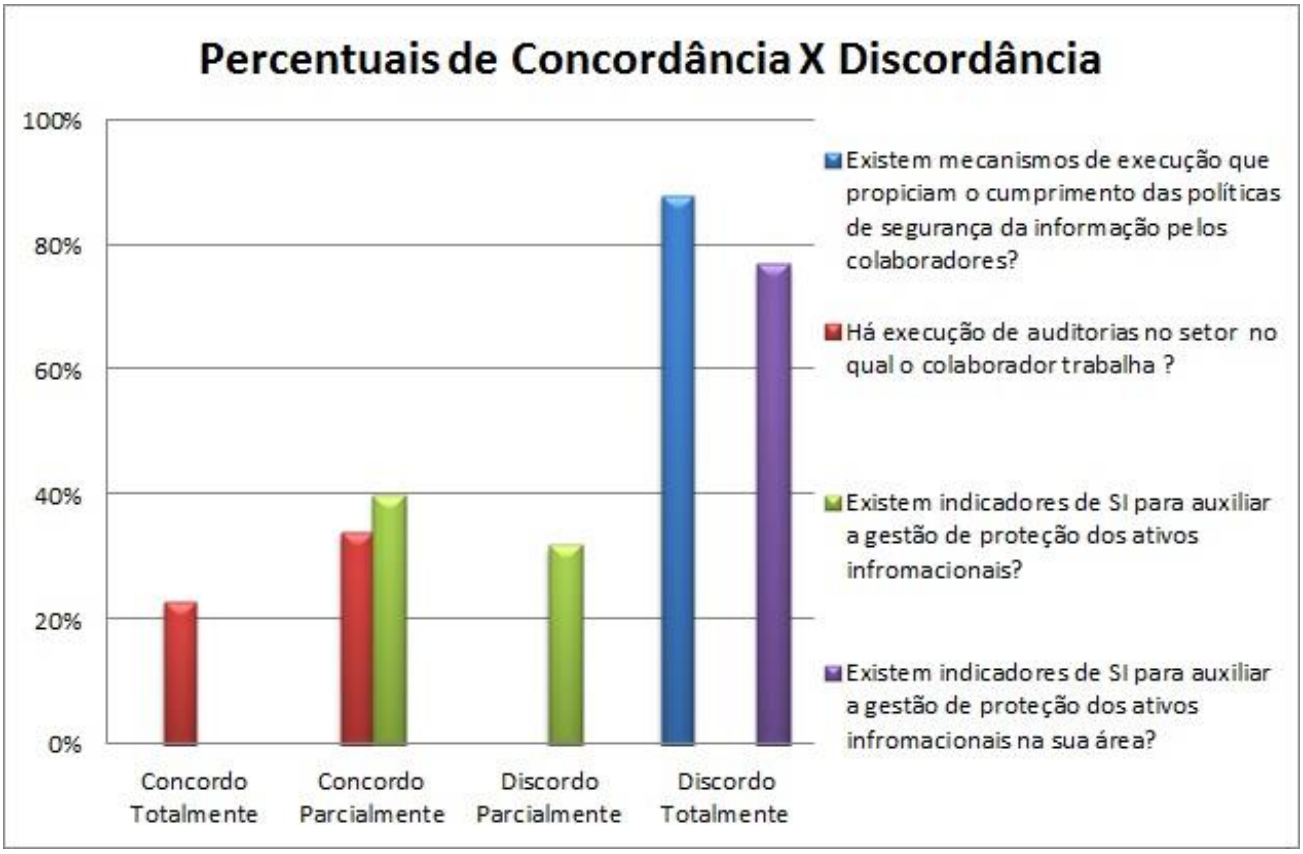
Inclusive, esse mesmo cenário é concretizado através da análise de resultados das respostas obtidas com a questão 31 que interroga o colaborador se existem mecanismos de execução que propiciam o cumprimento das políticas de segurança da informação pelos colaboradores. As respostas destacam que 88% dos respondentes discordam totalmente da afirmativa, demonstrando que há um cenário que requer a implementação de mecanismos que efetivem, regulem e controlem o cumprimento das políticas de segurança informacional instituídas na corporação.

Esses mecanismos são variados, porém na pesquisa há um referencial direto com relação à execução de auditorias (questão 16) no departamento ou setor ou área na qual o colaborador trabalha e quanto à existência de indicadores (questões 19 e 20) que venham a auxiliar os gestores na detecção de problemas de segurança informacional na organização. Antes de trazer as respostas obtidas, salienta-se que, durante as análises das políticas de segurança da informação disponibilizadas pela instituição, não houve nenhuma referência, nas políticas disponibilizadas, com relação a normas, políticas ou procedimentos que instituam e regulem as auditorias e como, onde, quando elas devem ser feitas. Destarte, acredita-se que elas ocorrem na instituição, haja vista que 57% dos respondentes concordam que há ocorrência de auditorias sobre segurança da informação em seu setor. Todavia, essa concordância é parcial, haja vista que 34% concordam parcialmente e 29% discordam parcialmente. Essa parcialidade nas respostas pode ser ocasionada exatamente pela falta de delimitação do assunto *auditorias* nas políticas de segurança da informação institucionais.

Já com relação aos indicadores, observa-se pelas respostas obtidas que parece haver indicadores de segurança da informação avaliados pela instituição. Todavia, não se trata de uma certeza concreta, haja vista que 40% dos colaboradores concordam parcialmente com a existência desses indicadores e 32% discordam parcialmente. Talvez esse seja um cenário que os colaboradores acreditam existir mas, que de alguma forma, ainda é intangível para eles. Essa intangibilidade pode ser percebida através das respostas à questão que avalia a presença de indicadores de

segurança da informação no setor ou área na qual o colaborador trabalha e 77% dos respondentes afirmam que não há a existência desses indicadores.

GRÁFICO 3:



Analisando a formação desse cenário com relação às políticas de segurança da informação, os recursos humanos e as tecnologias, tem-se um cenário composto de gargalos que precisam ser sanados. Os pilares de planejamento, organização, implementação e controle precisam ser sinérgicos, para que se consiga uma convergência e interação entre os elementos formais, informais e tecnológicos da empresa. Logicamente um plano de ação detalhado deve ser implementado incluindo, nesse caso, ações corretivas que devem ser praticadas desde já, visando a saúde de proteção dos ativos informacionais da empresa. Os indicadores de desempenho e as ações corretivas também são medidas de urgência que devem ser instituídas o quanto antes pela empresa.

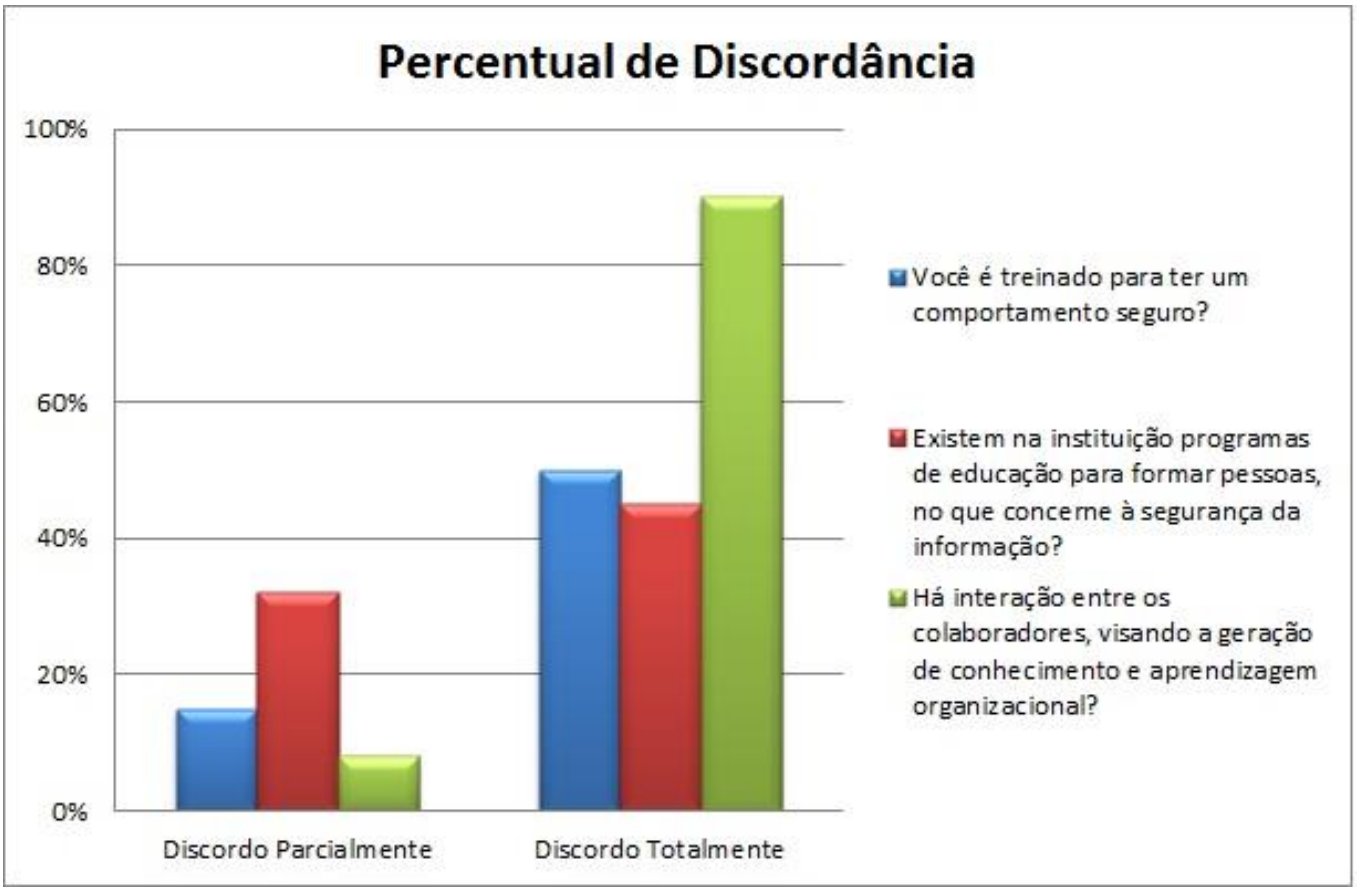
Entrando um pouco mais na percepção dos colaboradores com relação aos investimentos que são feitos pela empresa, sendo um montante maior para tecnologias e

menor para treinamentos de pessoas no que concerne à segurança da informação corporativa, a afirmativa 7 demonstrou que a grande maioria dos entrevistados, ou seja, 80%, têm a percepção de que a instituição investe mais em tecnologias do que em pessoas para garantir a segurança da informação empresarial. Quando são questionados se são treinados para terem um comportamento seguro, mais de 65% dos respondentes afirmam que não, observando-se que 50% deles tem total segurança de sua resposta (discordo totalmente). Esse parecer vem a se ratificar um pouco mais à frente no questionário, quando se pergunta aos colaboradores se existem na instituição programas de educação para formar pessoas, no que concerne à segurança da informação e 77% dos respondentes afirmam que não. Outro ponto importante de se mencionar é que 45% dos respondentes discordaram totalmente da afirmativa, ratificando com absoluta certeza que não se investe na formação do colaborador sob o aspecto da segurança informacional.

Respectivamente, as afirmativas 9 e 10 levantam reflexão à respeito da interação entre os colaboradores, visando a geração de conhecimento e aprendizagem organizacional. Destaca-se que houve mais de 90% de discordância, nenhuma resposta que concordasse totalmente e pouco mais de 8% que concordam parcialmente com a afirmativa 10, levando os pesquisadores a traçar um cenário no qual quase nunca ocorrem interações sociais com o objetivo de discutir a temática segurança da informação, ou seja, a instituição não tem aproveitado as ocorrências (ou fatos) do dia-a-dia para discutir de forma integrativa ações de segurança da informação.

Efetivamente há um cenário de desfavorecimento da interação nesse ambiente organizacional. A questão 24 questionou sobre o costume de se conversar, entre os próprios colaboradores, sobre incidentes de segurança informacional que tenham acontecido com eles próprios ou com algum conhecido. As respostas ratificam em parte o cenário da questão 10, demonstrando que apenas 34% dos respondentes concordam parcialmente, em um total de 51% de concordância, com a afirmativa que sugere que os colaboradores costumam conversar com os colegas sobre incidentes de segurança da informação ocorridos com eles ou com conhecidos.

GRÁFICO 4:



Nesse âmbito, traz-se a perspectiva apontada por Choo que a geração de conhecimento perpassa por quatro arenas, dentre elas a socialização. Não havendo socialização para discutir a segurança informacional das pessoas e da instituição, não há geração de conhecimento a partir da exploração dessa arena.

Curiosamente, quando comparamos os dados das afirmativas 9, 10 e 24, mais da metade dos respondentes (51%) discordam que as ações de segurança da informação implantadas na instituição geram conhecimento e promovem o aprendizado entre os colaboradores (afirmativa 9). E, apesar do total de 51% de discordância, 42% dos respondentes concordaram parcialmente e 5% concordam totalmente, quando refletem que as ações de segurança da informação implantadas na instituição geram conhecimento e aprendizagem organizacional.

Já quando são indagados se têm oportunidade de sugerir ações de segurança informacional, 57% afirmam que sim, concordando com a questão. Muito embora concordem que têm oportunidade de sugerir ações de segurança da informação na

instituição (afirmativa 25), entre eles, metade concordaram parcialmente, ou seja, mesmo entre os concordantes observa-se uma dificuldade para realizar as sugestões.

A comparação desses dados (afirmativas 9, 10, 24 e 25) demonstra discrepância de opiniões ou medo quando indagados mais profundamente sobre o tema – segurança da informação - aplicado à instituição na qual trabalham os respondentes. Apesar do anonimato do questionário e das respostas não passarem pela instituição, haja vista que foram diretamente para um banco de dados virtual ao qual somente o pesquisador tem acesso, sabe-se que quando o tema é segurança da informação muitos ainda possuem receio de falar abertamente.

Unindo as análises dessa primeira etapa, há a percepção de que ocorre um desequilíbrio entre os pilares *pessoas, processos* e *tecnologias*, demonstrando um cenário tendencioso a uma abordagem tecnicamente orientada na instituição pesquisada.

6.2 - Cenário Comportamental dos colaboradores

O primeiro fator direcionador de comportamento seguro é entender se os colaboradores conhecem e compreendem as políticas, procedimentos, normas e diretrizes de segurança da informação adotadas pela instituição. Os dados demonstram um equilíbrio muito grande entre concordâncias (51%) e discordâncias (48%), sendo que quando os dados são desdobrados, observa-se que os maiores percentuais estão em concordo parcialmente (40%) e discordo parcialmente (31%). Outro fator que auxilia na reflexão da efetividade das políticas de informação é entender se os colaboradores consideram volumosa ou não a quantidade de normas, diretrizes e procedimentos que eles devem cumprir. Nesse sentido, observa-se que há um consenso e que 77% discordam da afirmação, expondo que as políticas não são volumosas, porém a maioria dos respondentes (69%) alegam, através de sua discordância na questão 26, que as políticas de segurança da informação instituídas pela organização não são de fácil compreensão. Outro ponto interessante é que, apesar de todo o cenário traçado até agora no que concerne à segurança da informação e sua aplicação nas políticas de segurança informacional da instituição pesquisada, 77% das respostas obtidas indicam que os colaboradores têm consciência que devem cumprir todas as políticas de segurança da

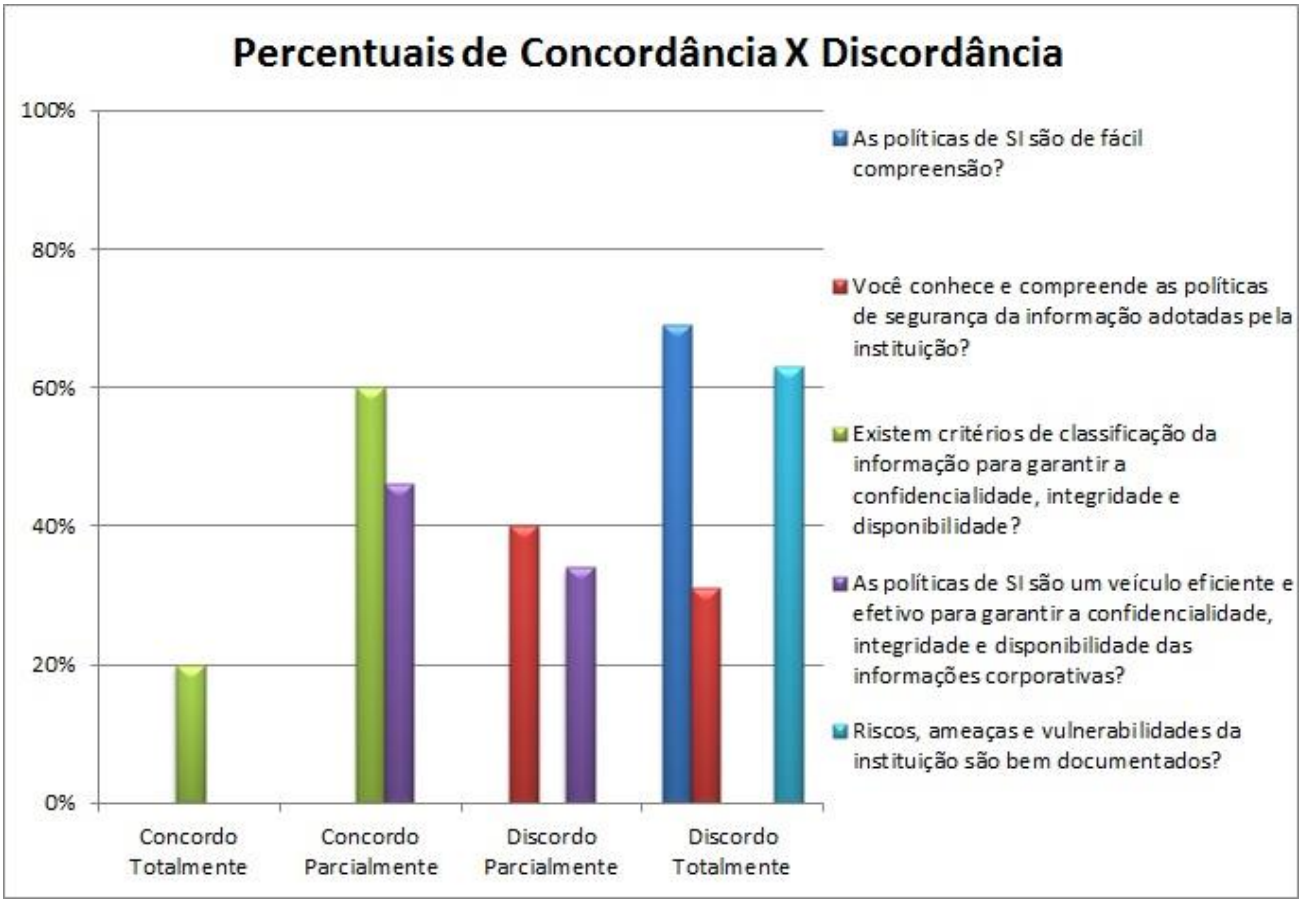
informação instituídas e não escolher algumas ou as que consideram mais fáceis para cumprir. Entretanto, apesar da existência de uma política determinando a necessidade de se fazer *backups* frequentes dos dados e informações contidos em máquinas e equipamentos, quando questionados sobre a existência de orientação ou obrigação para fazer back-ups diários das informações processas pelo usuário, 74% dos respondentes discordam da afirmativa, ou seja, não se sentem orientados e nem obrigados a fazer *backups*. Mais um elemento que indica a necessidade de equilíbrio de investimentos das organizações entre as variáveis formais, informais e tecnológicas da empresa. De que adianta investir maciçamente em tecnologias se o usuário permitir a entrada de um intruso nas bases de dados da empresa? De que adianta a maior segurança tecnológica se os usuários não fazem backups? De que adianta uma fortaleza tecnológica digital e física se os seres humanos que transformam os dados e informações não se importarem efetivamente com a proteção dos ativos informacionais da empresa? Talvez um dos caminhos seja olhar para pessoas, processos e tecnologias de forma equitativa e equilibrada.

Esse cenário demonstra que, apesar de serem de bom tamanho, as políticas não possuem interface amigável e didática aos olhos dos colaboradores, fato este que pode ser um dos motivos para que os colaboradores conheçam parcialmente essas políticas de segurança da informação da instituição. Todos os fatores que geram entrave ao entendimento do colaborador sobre como agir, mesmo ele tendo consciência de que é um de seus deveres seguir as políticas de informação da empresa, pode ter um efeito negativo em seu comportamento informacional, especialmente em situações de perigo, como no caso de incidentes de segurança da informação. O fato dos colaboradores não estarem totalmente seguros com relação ao seu conhecimento no que concerne às políticas, normas, procedimentos e diretrizes de segurança da informação adotadas pela instituição, gera um *gap* na gestão da informação e conhecimento, na eficácia das políticas e, principalmente, um reflexo negativo na aprendizagem organizacional.

Essa falta de conhecimento reflete diretamente no comportamento do colaborador, haja vista que a maior parte dos respondentes disseram que não conseguem entender através das regras de segurança da informação disponibilizadas pela instituição, ou seja, políticas, normas, procedimentos e diretrizes de segurança informacional, qual deve ser o comportamento que a empresa espera que seu colaborador tenha. Em um mundo globalizado e dinâmico, os incidentes de segurança

da informação não param de acontecer. Quando uma pessoa sofre uma ameaça e possui informação e conhecimento sobre como agir, sua reação tem mais parâmetros. Agora, quando se sofre ameaças e não há informações e conhecimento que formulem parâmetros de como agir, as ameaças interceptam um indivíduo de modo muito mais vulnerável e que cujas reações serão muito mais previsíveis. Por isso que a maior parte dos respondentes (63%) discordam quando indagados sobre o fato dos riscos, ameaças e vulnerabilidades da instituição serem bem documentados. Analogamente, a maior parte dos colaboradores concorda parcialmente (45%) e discorda parcialmente (23%) quando questionados se os mesmos riscos, ameaças e vulnerabilidades são comunicados pela instituição aos colaboradores. Concomitantemente 80% dos respondentes concordam, mesmo que o percentual majoritário (60%) concorde parcialmente, que o desenvolvimento da segurança da informação na instituição na qual trabalham inclui proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo, sejam elas internas e/ou externas à organização.

GRÁFICO 5:



A instituição pesquisada possui, exploratoriamente, um déficit no quesito gestão da informação e do conhecimento na ótica da segurança da informação. Assim, 68% dos seus colaboradores que sofrem ameaças de segurança informacional têm seu comportamento alterado devido a essas vivências. Nota-se que esses funcionários poderiam ter seu comportamento alterado devido ao conhecimento e à preparação que possuem, e, não adquirir conhecimento em um formato de ação e reação. Esse cenário demonstra fragilidade de posicionamento das políticas organizacionais e da instituição em si, frente aos recursos humanos e frente a uma abordagem holística e sistêmica relativa à segurança da informação corporativa.

Os incidentes de segurança da informação podem ser derivados de invasões na máquina ou equipamento no qual se processa as informações, contudo, muitas das vezes essa invasão tem a permissão, intencional ou não, do usuário. Observa-se que 89% discordam que postem em redes sociais fatos ou ocorrências que acontecem na organização ou no setor para alertar amigos (afirmativa 41). Não obstante, 9% dos respondentes afirmaram que fazem essas postagens. Percebe-se que, por falta de definição do comportamento que a empresa espera do colaborador em relação à segurança da informação, algumas informações relevantes ou estratégicas de fragilidade do sistema da empresa podem estar sendo compartilhadas com pessoas estranhas ao ambiente institucional, gerando verdadeiras ameaças aos ativos informacionais da empresa.

6.3 - Cenário de Déficit Comunicacional

Outro ponto importante de se mencionar é o déficit comunicacional da empresa, no que concerne às informações sobre segurança informacional. Na afirmativa 15, identificou-se uma deficiência na comunicação entre empresa e trabalhadores, uma vez que menos da metade dos trabalhadores afirmaram ter ciência de todas as atualizações de avaliação de riscos de seu departamento, setor ou área.

Apesar desse cenário de valorização da tecnologia e de desfavorecimento do elemento humano, nota-se que 65% dos respondentes têm interesses em absorver os valores, missão e visão da empresa para a qual trabalham, contra 35% que concordaram

que, em primeiro lugar, dedicam atenção à sua profissão e à especialidade do computador com o qual trabalham, para depois absorver os valores, missão e visão da empresa. Deve-se dedicar especial atenção a esse fator, uma vez que 72% dos respondentes concordaram ou discordaram parcialmente da afirmativa, podendo ser um indicativo que o elemento *pessoas* precisa de atenção devida para que haja efetividade nas ações de segurança da informação da instituição.

Complementar a essa visão, apesar de 63% dos respondentes considerarem que o ambiente da empresa é seguro no que concerne às informações que nele são processadas (afirmativa 50), 9% dos respondentes sentem vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é a segurança da informação da instituição. E 58% dos respondentes se sentem prejudicados pela alta carga de trabalho imposta pela instituição, indicando que esse fator os prejudica com relação à percepção e ações relativas à segurança da informação.

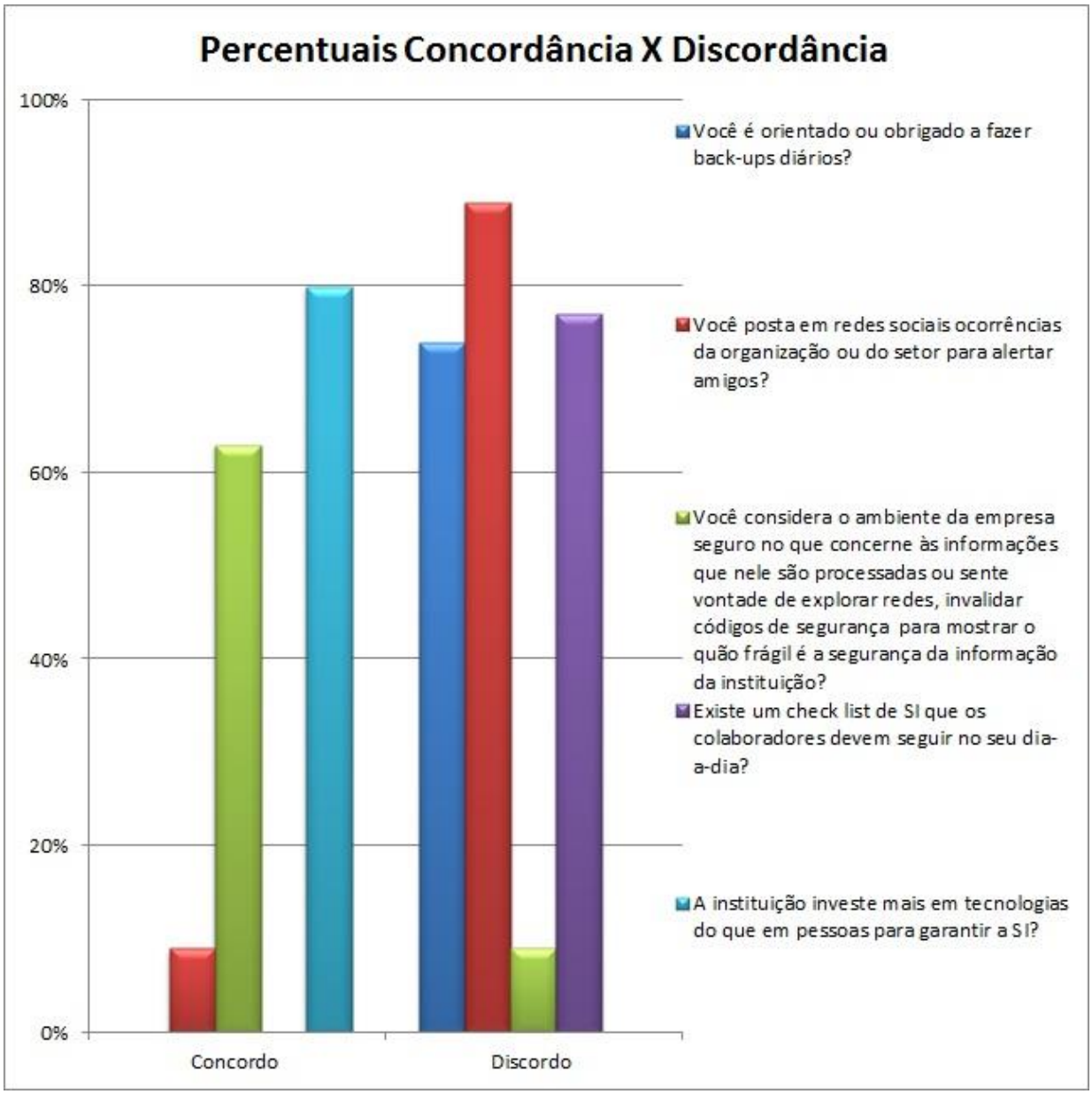
Considerando o exposto acima e os valores das médias da escala Likert para cada afirmativa, identifica-se que, embora os colaboradores se sintam parte responsável pela segurança da informação (afirmativa 5, média 3,8), entendam o que é segurança da informação (afirmativa 3, média 3,8), não tenham intenção de explorar a rede, invalidando códigos e expondo fragilidades (afirmativa 43, média 3,7) e identifiquem quem são as pessoas responsáveis pela informação (afirmativa 17, média 3,2), falta interação entre os colaboradores para discutir temas de segurança da informação (afirmativa 10, média 1,4), programas de educação para formar pessoas com relação à segurança da informação (afirmativa 48, média 1,8) e mais investimento em treinamentos para os colaboradores (afirmativa 7, média 1,9).

6.4 - Cenário de informações relativas à tecnologia

Com relação ao fato da instituição permitir o acesso à rede corporativa, para gravar dados em pen-drives, CD´s, DVD´s e/ou imprimir informações para uso tanto no ambiente institucional quanto em casa (questão 34), 80% dos respondentes discordaram enfatizando que essas não são ações permitidas. Os mesmos 80% dos respondentes

observam, ao utilizar o e-mail corporativo, a supressão de mensagens que possuem anexos não solicitados (questão 33). Concomitante, não há acesso irrestrito a sites (questão 36) de acordo com 80% dos respondentes e nem permissão de acesso remoto a sistemas de informação corporativos, de acordo com 75% dos respondentes.

GRÁFICO 6:



Vinculando a parte tecnológica com as políticas de segurança da informação da empresa observa-se, conforme 77% dos respondentes afirmam, não existe um *check list* de segurança informacional que os colaboradores devem seguir no seu dia-a-dia. Já

com relação à alteração mensal das senhas de acesso aos recursos corporativos, 65% dos respondentes concordam com a afirmativa, todavia, 37% desses concordam parcialmente.

A leitura final por agrupamentos mostra que o agrupamento “Pessoas” apresentou média de 2,5, o agrupamento “Processos” média de 2,7 e o agrupamento “Tecnologia” média de 2,8.

Para verificar se os escores totais de cada agrupamento diferiam em parâmetro de localização, ou seja, se um agrupamento tende a apresentar valores superiores (ou inferiores) aos outros, realizou-se o teste de Kruskall-Wallis, que é um teste alternativo ao teste T.

O valor de teste obtido foi KW=0,293, p-valor=0,864, não rejeita a hipótese de igualdade entre os escores totais de cada agrupamento, ou seja, não há evidência amostral que um agrupamento tenha escores totais maiores que os demais.

7 - Considerações Finais

A segurança da informação foi pesquisada sobre o ponto de vista gerencial, envolvendo questões como as fontes de informações corporativas, as necessidades de uso da informação por usuários corporativos e as diretrizes corporativas que permeiam toda a vida da organização. Descreveram-se, exploratoriamente, as variáveis envolvidas na criação de um comportamento seguro para o usuário da informação, bem como a segurança da informação sob o ponto de vista da gestão de recursos humanos, de processos e tecnologias. Dessa forma, concluiu-se que a importância da educação e do aprendizado organizacional nas questões de segurança da informação é fundamental. Finalmente, foram apresentados resultados da pesquisa, enfatizando a tríade *pessoas*, *processos* e *tecnologias* e segurança da informação em uma empresa do ramo de saúde.

As pessoas estão presentes em todos os locais, e são esses os recursos organizacionais que transformam os dados em informações e que possuem contato direto com o ativo informacional corporativo. Entretanto, cabe aos recursos humanos organizacionais atentar para políticas e diretrizes organizacionais criadas para manter a segurança. E cabe, simultaneamente à organização e ao seu corpo gerencial, tornar tais políticas e diretrizes conhecidas e valorizar sua adoção.

Empresas de saúde, conforme mencionado nessa pesquisa, são organizações em que a informação médica de pessoas circula livremente em sistemas. Tal circulação ocorre intra e extraorganização, uma vez que outras empresas parceiras comerciais e seus colaboradores podem ter acesso a informações sigilosas relativas à saúde de terceiros. Esse caso se torna ainda mais critico em instituições de saúde pública, que muitas vezes lidam com a produção de informação médica através da oferta de serviços de saúde. Nesses casos, cabe também uma abordagem, como a aqui sugerida, que extrapole as fronteiras dos departamentos de tecnologia da informação.

Nesse sentido, observa-se que as organizações devem examinar constantemente seus processos, no sentido de verificar se pessoas, processos e tecnologias estão recebendo incentivos e desenvolvimento de ações equitativos, de modo a atender uma abordagem sistêmica para a gestão de segurança informacional.

Através de um instrumento de coleta de dados com consistência interna comprovada estatisticamente, há possibilidade de se aplicar pesquisas no sentido de

avaliar o comportamento das pessoas e como elas estão agindo frente às ações de segurança da informação, promovidas pela instituição, e se as políticas de informação em vigor tem o impacto esperado sobre variáveis pré-determinadas. Destarte, verifica-se, nesse momento, se há nessa interação nas relações e condutas das pessoas, brechas para ocorrência de incidentes de segurança informacional que venham a delinear um cenário de comportamento inseguro por parte dos recursos humanos. A partir do cruzamento das variáveis componentes do instrumento de coleta de dados, há possibilidade de se explorar porquê alguns elementos são potenciais geradores de falhas de segurança informacional, delinear os cenários dessas ocorrências, entender como lidar com as circunstâncias de falhas de segurança e desenvolver planos de ações para corrigir e prevenir futuros incidentes.

Essas etapas foram percorridas na prática durante o trabalho de campo dessa pesquisa que, através do uso do instrumento de coleta de dados e da metodologia proposta, conseguiu delinear para a empresa pesquisada quais são as brechas para ocorrência de incidentes de segurança da informação, de modo a contemplar um possível cenário de comportamento inseguro.

Outro ponto que é objeto de resultados específicos dessa pesquisa é a contextualização da Segurança da Informação como temática relevante no campo da Ciência da Informação. Entende-se que esse objetivo foi alcançado, uma vez que o objeto passível de segurança nas organizações é a informação que é o elemento central da ciência da informação no âmbito das ciências sociais aplicadas. Ao sugerir uma abordagem sistêmica para a segurança da informação corporativa, instituiu-se que um dos elementos geradores de falha de segurança seja o usuário da informação, exatamente aquela pessoa que necessita, utiliza, transforma e agrega valor à informação com finalidades específicas.

Retomando o trabalho de campo realizado, agora no sentido de se medir as ações tomadas pela instituição pesquisada no âmbito da segurança informacional, gerou, como resultados, a abordagem tecnicamente orientada instituída na organização que não contempla com equidade os elementos *pessoas, processos* e *tecnologias*. Outro fator que também ficou claro nos resultados da pesquisa é que as falhas de segurança informacional podem estar vinculadas à falta de interação entre as três arenas e à falta de gestão estratégica de segurança informacional que seja contemplada desde o planejamento estratégico da instituição. Efetivamente, os resultados da pesquisa

demonstram que seus usuários da informação estão pouco preparados para agir seguramente e que as falhas de segurança da informação estão vinculadas à falta de uma gestão estratégica de segurança informacional que englobe, sumariamente, as ações de segurança no aprendizado organizacional, gestão da informação e do conhecimento, aquisição de conhecimento com vistas à mudança comportamental dos colaboradores da instituição, educação e a gestão de capital intelectual.

A inter-relação entre o usuário da informação e a segurança informacional institucional deve ser monitorada constantemente, para que se consiga agir antecipadamente frente à dinâmica dos incidentes de segurança. Como demonstrado na pesquisa de campo, uma das formas de se checar e controlar essa inter-relação é através da medição constante das ações de segurança informacional implementadas e a reação dos colaboradores frente a elas. Essa medição mostrará o cenário da instituição e que ajudará as organizações a se prevenir dos incidentes de segurança informacional, especialmente aqueles que envolvem pessoas.

Através da avaliação descritiva dos dados e da discussão dos resultados, pode-se concluir que o elemento pessoas é uma variável crítica na gestão de segurança informacional nas organizações. As políticas de informação devem ser acessíveis aos funcionários e factíveis de serem executadas. Com relação à tecnologia, é válido que continuem os investimentos, entretanto eles devem ser equilibrados com o desenvolvimento de controles informais (*pessoas*) e controles formais (*políticas* e *processos*) para que haja uma gestão de segurança informacional mais efetiva e eficaz.

Como fatores limitadores da pesquisa destaca-se o número de respostas obtidas na aplicação do instrumento de coleta de dados. O questionário dispunha de 51 perguntas e, dado o fato de se ter obtido apenas 35 respostas em um universo de 100 possíveis respondentes, esse fator prejudicou a capacidade de generalização do instrumento de coletas de dados.

Desse modo deixa-se como sugestões para futuras pesquisas a aplicação do instrumento de coleta de dados desenvolvido nessa pesquisa em uma amostra maior que 51 respondentes e a releitura, a partir dos novos dados, da validação do questionário principalmente no que concerne à capacidade de generalização.

8 – Referências Bibliográficas:

ALLEN, B. L. *Information Tasks: Toward a User-centered approach to information systems.* USA, Academic Press, California, 1996.

ALMEIDA, M. B. *Aplicação de Ontologias em Segurança da Informação*. Belo Horizonte: Editora Fonte, 2007.

ALMEIDA, M. B., SOUZA, R. R., COELHO, K. *Uma proposta de ontologia de domínio para segurança da informação em organizações:descrição do estágio terminológico.* Revista: Inf. & Soc.:Est., João Pessoa, v.20, n.1, p. 155-168, jan./abr. 2010

ALVARENGA NETO, R. C. D. *Gestão do conhecimento em organizações: proposta de mapeamento conceitual integrativo.* São Paulo: Saraiva, 2008. 236p.

ANDALÉCIO, A. L.; SOUZA, R. R., *Ciência Cognitiva e Ciência da Informação*: Paralelos. Londrina, jan./jul., 2008, v.13, n.1, p.72- 80.

BABBIE, E. *Métodos de Pesquisa Survey.* Tradução de Guilherme Cezarino. Belo Horizonte: UFMG, 1999. 519 p. (Coleção Aprender).

BARBETTA, P. A. Estatística Aplicada às Ciências Sociais. Santa Catarina: Editora UFSC, 2007, 7ª edição.

BARBOSA, R. R. *Inteligência Empresarial: uma avaliação de fontes de informação sobre o ambiente organizacional externo.* Data Grama Zero, 2002, v. 3, n.6, p. 42-53. Disponível em: http://www.dgz.org.br/dez02/Art_03.htm, acesso em: 10/12/2011

BARBOSA, R. R. *Gestão da informação e do conhecimento: origens, polêmicas e perspectivas.* Londrina, 2008, v. 13, n. esp., p. 1-25.

_____. Uso de fontes de informação para a inteligência competitiva: um estudo da influência do porte das empresas sobre o comportamento informacional. *Revista eletrônica de Biblioteconomia e Ciência da Informação*. Número especial, Florianópolis: Revista Eletrônica de Biblioteconomia e Ciência da Informação, 1o sem. 2006. Cap. 91. p. 91-102.

BARBOSA, R. R.; PAIM, I. Da GRI à gestão do conhecimento. In: PAIM, I. (org.). *A Gestão da Informação e do Conhecimento.* Belo Horizonte: Escola de Ciência da Informação da UFMG, 2003.

BARBOSA, R. R. Monitoração Ambiental: uma visão interdisciplinar. *Revista de Administração*, 1997. v. 32. n. 4, p. 42-53.

BARRETO, A. A *et al*. *Gestão estratégica da informação e inteligência competitiva*.SP, Saraiva, 2006. p. 3-351.

BEAUTEMENT, A.; SASSE, A. *The economics of user effort in information security*. ComputerFraud & Security, 2009.

BEAVER, K. *Healthcare information systems.* A CRC Press Company, 2003. 2nd edition.

BERGER, P.; LUCKMANN, T. *A construção social da realidade*. Rio de Janeiro: EditoraVozes, 1999.

BLACK, A. *Information History.* ARIST. 2006. v.40, n.1, p.441-473.

BMF BOVESPA. Disponível em: http://www.bmfbovespa.com.br/pt-br/intros/intro-servicos-de-informacao.aspx?idioma=pt-br. Acesso em: 17 de julho de 2011.

BORKO, H. *Information Science; what is it? American Documentation*, v.19, n.1, p.3-5, jan. 1968.

BRAMAN, S. *Defining information: an approach for policymakers. Telecommunications Policy.* Sept. 1989. v. 13, n. 3, p. 233–242. http://www.uwm.edu/?braman/bramanpdfs/ defining.pdf>. Acesso em: 11 de ago de 2011.

BRASIL. República Federativa do. *Decreto nº 3.505, de 13 de junho de 2000.* política de segurança da informação nos órgãos e entidades da Administração Pública Federal, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 14 jun. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em 26 de outubro de 2010.

BRASILEIRO, A. M. M. Métodos e Técnicas de Pesquisa. (Desenvolvimento de material didático ou instrucional - Elaboração de material para disciplina em EAD), Belo Horizonte, UniBH, 2011. (temos que trocar na dissertação Brasileiro 2012 por brasileiro 2011)

BRAVERMAN, H. *Trabalho e capital monopolista: a degradação do trabalho no século XX*. Rio de Janeiro: Zahar, 1977.

BROWNE, M. *The field of information policy: 1. Fundamental concepts*. Journal of Information Science. Agosto 1997, n. 23, p. 261-275

BROWNE, M. *The field of information policy: 2. Redefining the boundaries and methodologies*. Journal of Information Science. Outubro 1997, n. 23, p. 339-351

BRUM, M. A. C.; BARBOSA, R. R. *Comportamento de busca e uso da informação: um estudo com alunos participantes de empresas juniores.* Revista Perspectivas em Ciência da Informação, v. 14, n.2, 2009. Belo v. 14, n. 2, p. 52-75. Editora ECI/UFMG, 2009.

BRUM, M. A. C. BARBOSA, R. R. *Uso de fontes de informação para a inteligência competitiva: um estudo sobre a influência do porte das empresas sobre o comportamento informacional.* Enc. Bibli: R. Eletr. Bibliotecon. Ci. Inf., Florianópolis, n. esp., 1º sem. 2006, p.91-102.

BUCKLAND, M. *Information as a thing. Journal of American Society for Information Science*, 1991, v. 42, n. 5, p. 351-360.

BUSH, V. As We May Think, in The Atlantic Monthly, Julho, 1945. Disponível em: http://ccat.sas.upenn.edu/ jod/texts/vannevar.bush.html,
e http://www.theatlantic.com/unbound/flashbks/computer/bushf.htm,
Acesso em 23/08/11

CAPURRO, Rafael Epistemology and Information Science. Royal Institute of Technology Library, Stockholm, August 1985, Report TRITA-LIB-6023. Online: http://www.capurro.de/trita.htm

CASSIANI, S. de B.; CALIRI, M.H.L.; PELÁ, N.T.R. A teoria fundamentada nos dados como abordagem da pesquisa interpretativa. *Revista latino-americana de enfermagem*, 1996, v. 4, n. 3, p.75-88.

CASTELS, M. A sociedade em rede. São Paulo: Paz e Terra 1999, 620p.

CENDÓN, B. V. et al. *A Gestão da Informação e do Conhecimento*. Belo Horizonte: Escola de Ciência da Informação / UFMG, 2003.

CHOO, C. W. *A organização do conhecimento*. São Paulo: SENAC, 2006. 2a. ed.

CHOO, C. W.; BERGERON, P.; DETLOR, B.; HEATON, L. *Information culture and information use: an exploratory study of three organizations.* Journal of the American Society for Information Science and Technology, 2008. v. 59, n. 5, p. 792-804.

COLWILL, C. R. *Human factors in information security: The insider threat & Who can you trust these days?* Information Security Technical Report, 2010, p. 01-11.

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

DAVENPORT, T. H. Processos de gerenciamento da informação. In: ____. *Ecologia da informação.* São Paulo: Futura, 2001. Cap.8.

DAVENPORT, T. H.; PRUSAK, L. *Conhecimento empresarial: como as organizações geram seu capital intelectual.* Rio de Janeiro: Campos, 1998.

DAVENPORT, T. H. *Reengenharia de Processos.* Rio de Janeiro: Editora Campus, 1994.

DAVENPORT, T. H. *Ecologia da Informação*. São Paulo: Futura, 2002. 316 p.

DAVENPORT, T. H.; PRUSAK, L. *Ecologia da Informação: por que só a tecnologia não basta para o sucesso na era da informação.* São Paulo: Futura, 1998. 5. ed.

DRUCKER, P. *O gerente eficaz.* Rio de Janeiro: Guanabara Koogan, 1990.

DRUCKER, P. *The information executives truly needs.* New York: Harvard Business Review. jan-feb.1995. v.73, n.1, p.54-62.

DRUCKER, P. *The comming of the new organization.* Boston: Harvard Business Review. jan-feb.1988. v.88, n.1, p.45-53.

DRUCKER, P. *A quarta revolução da informação.* São Paulo: Exame. .ago.1998. v.32, n.18, p.56-58.

DUPAS, G. Economia Global e Exclusão Social: pobreza, emprego, estado e o futuro do capitalismo. 3ª ed. revista e ampliada. São Paulo: Paz e Terra, 2001.

EIU. *The Economist intelligence Unit: Power to the people? Managing technology democracy in the workplace*, http://graphics.eiu.com/marketing/pdf/Technology%20Democracy.pdf; June 2009.

EVERETT, C. *Cover Story: Education, Education, Education.* Infosecurity. 2008. n.6, v.5, p. 14-18

FERREIRA, A.; Antunes, L.; Chadwick, D.; Correia, R. *Grounding Information Security in Healthcare.* International Journal of Medical Informatics. 2010. n.70, p.268-283.

FIBIKOVA, L., VYSKOC, J. *IT users' perception of information security. In: 2nd Working Conference on Security and Control of Information Technology in Security*, Bratislava: Comenius University, 107, 2001.

FRANÇA, J. L. et al. *Manual para normalização.* Belo Horizonte: Editora UFMG, 2004. 7a ed.

GHERNAOUTI-HÉLIE, S. *An inclusive information society needs a global approach of information security. International Conference on Availability, Reliability and Security.* Computer Society, 2009.

GÓMEZ, M. N. G. Metodologia de pesquisa no campo da Ciência da Informação. DataGramaZero - *Revista de Ciência da Informação*. dez 2000. vol. 1, n. 6.

GOODMAN, K. *Ethics, Computing and Medicine*.Cambridge: University Press, 1998.

GRITZALIS, D. *A baseline security policy for distributed healthcare information systems.* Computer & Security. Elsevier, 1997. n.8, v.16, p.709-719.

GRUNIG, J. E. (1997). *A situational theory of publics: conceptual history, recent challenges and new research.* In D. Moss, T. MacMannus, & D. Vercic (Eds). Public relations research: An international perspective (pp. 3-48). London: International

Thomson Business Press.

GUNTHER, H. *Pesquisa Qualitativa versus Pesquisa Quantitativa: É esta a questão?* Psicologia: Teoria e Pesquisa, vol.22, n.2, Brasília, 2006, pp. 201-210

HAIR, J. F. [et al.]; Análise Multivariada de Dados. 6º ed. - Porto Alegre: Bookman, 2009.

HAYEK, Friedrich A. *The Use of Knowledge in Society.* American Economic Review. XXXV, No. 4. pp. 519-30. American Economic Association . 1945 . Library of Economics and Liberty [Online] available from http://www.econlib.org/library/Essays/hykKnw1.html; Acesso em 07 de março de 2011; Internet.

HERSH, W. R. *Information retrieval: a health and biomedical perspective.* New York: Springer-Verlag. 2003. 2nd edition.

HONE, K.; ELOFF, J.H.P. *Information security policy – what do international information security standards say?* Elsevier Science, 2002, p. 402-409

HUANG, D. L.; RAU, P. L. P. & SALVENDY, G. *Perception of information security.* Behavior & Information Technology, 2010. v.29, n.3, p. 221- 232.

INGWERSEN, P. *The cognitive view and information.* In: _____. **Information retrieval interaction**. London: Taylor Graham Publishing, 1992. Chapter 2. Disponível em: <http://vip.db.dk/pi/iri/files/Ingwersen_IRI_Chapter2.pdf>. Acesso em: 8 mar. 2010.

ISO/IEC 15408-1. *Internacional Standard – Information Technology – Security Techniques (2005).* http://www.iso.org. Acesso em: 21 de Abril 2010.

JONES, W. *Personal Information Management*. ARIST, v.41, n.1.

KAVANAGH J. *Security special report: the internal threat*, Computer Weekly, 25/4/06, http://www.computerweekly.com/Articles/ 2006/04/25/215621/security-special-report-the-internal-threat.htm; 2006. Acesso em 03/03/2010.

KEBEDE, G. *Knowledge management: An information science perspective.* International Journal of Information Management, 2010.

KARAKAS, F. *Welcome to world 2.0: the new digital ecosystem. Journal of Business Strategy*, 2009, p. 23.

KIMBLES, S. The *Cultural Complex and the Myth of Invisibility* In: SINGER, Thomas (Org). **The vision thing**: myth, politics and psyche in the world. London: Routledge, 2000. p. 213-231.

KOSKOSAS, I. V.; CHARITOUDI, G.; LOUTA, M. *The role of organizational cultures in information-systems security management.* Journal of Leadership Studies. Spring, 2008. v.2, issue 1, p.7–17.

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

LACEY, D. *Managing the human factor in information security*. Wiley. 2009.

LEGEY, L-R. e ALBAGLI, S. *"Construindo a sociedade da informação no Brasil: uma nova agenda".* DataGramaZero – Revista de Ciência da Informação, v.1, n.5, out. 2000. Disponível em: <http:/ /www.dgz.org.br>.

MALHOTRA, N. K. *Pesquisa de Marketing: Uma Orientação Aplicada*, Porto Alegre: Bookman, 2012, 4a edição.

MARCIANO, J. L. P. *Segurança da Informação: uma abordagem social. Dissertação* (Doutorado em Ciência da Informação). Brasília: Universidade de Brasilia. 2006.

MARCHIONINI, G. *Digital Library Research and Development.* Encyclopedia of Library and Information Science, 1998, v.63

MCGEE, J.; PRUSAK, L. *Gerenciamento Estratégico da Informação: Aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica*. Rio de Janeiro: Campus, 1994. 7a. ed.

MEADOW, C. T. *Text information retrieval systems*. San Diego. 1992.

MEDEIROS, J. B. *Redação Científica: A prática de fichamentos, resumos, resenhas*. São Paulo: Editora Atlas, 1997. 3a. ed.

MORAES, R. *Análise de conteúdo*. Porto Alegre: Revista Educação, 1999. v. 22, n. 37, p. 7-32.

NARITA, T.; KITAMURA, Y. *Persuasive Conversational Agent with persuasion tactics.* LNCS 6137. Springer-Verlag Berlin Heidelberg, 2010, p.15-26

NEHMY, R. M. Q.; PAIM, I. *Gestão do Conhecimento, "Doce Barbárie"?*. In: A Gestão da Informação e do Conhecimento. Belo Horizonte.. Escola de Ciência da Informação – UFMG. 2003.

NIAC. HMG IA standard No. 1, *technical risk assessment part 1* (Issue 3.2); October 2008.

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC). *Final report and Recommendations:the insiderthreat tonational infrastructures,* 8/4/08, http://www.dhs.gov/xlibrary/assets/niac/niac_insider_ threat_to_critical_infrastructures_study.pdf; 2008.

NIEKERK, J.F.V.; SOLMS, R.V. *Information Security Culture: A management perspective.* Computer & Security. 2010. n4.v.29, p.476.

NONAKA, I. & TAKEUCHI, H.. *Criação de Conhecimento na Empresa: Como as Empresas Japonesas Geram a Dinâmica da Inovação*. Rio de Janeiro: Campus. 1997.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Guidelines for the security of information systems and networks: towards a culture of security*. Paris: 2002. Disponível em: <http://www.oecd.org/dataoecd/16/22/ 15582260.pdf>. Acesso em: 02. dez. 2010.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). *Guidelines for the Security of Information Systems*. (1992). Available from Internet: <http://www.oecd.org/ >. Paris. 2002. Acesso em: 02 de Dezembro 2010.

PASQUALI, L. *Análise descritiva dos dados de pesquisa*. Disponível em: http://www.psi-ambiental.net/pdf/PasqCap02.pdf. Acesso em: 06/08/2011

PERELMAN, C. *La Classification dans les Sciences - Réflexions Philosophiques sur la Classification.* Centre National de Recherche de Logique / Société Belge de Logique et Philosophie des Sciences (ed.), Bruxelles: Éditions J. Duculot S.A. Gembloux. 1963, p.231- 236.

PEREIRA, F. C. M. *Uso de fontes de informação: um estudo em micro e pequenas empresas de consultoria de Belo Horizonte*. (2006). Dissertação (Mestrado em Ciência da Informação) - Belo Horizonte: Escola de Ciência da Informação, Universidade Federal de Minas Gerais. 2006.

PEREIRA, J. C. L. *Necessidades, busca e uso da informação: Estudo de caso em um setor de help desk de indústria cimenteira multinacional.* Dissertação (Mestrado em Ciência da Informação.) - Belo Horizonte: Escola de Ciência da Informação, Universidade Federal de Minas Gerais. 2008.

PESTANA, Maria Helena, GAGEIRO, João Nunes. Análise de dados para ciências sociais – A complementaridade do SPSS. Lisboa. Silabo, 1998.

PINHEIRO, L. V. R., *Informação: esse obscuro objeto da ciência da informação.* Morpheus, v. 2, n. 4, 2004. Disponível em: <http://www.unirio.br/morpheusonline/Numero04-2004/lpinheiro.htm>. acesso em 02/06/2011.

PINHEIRO, L. V. R., LOUREIRO, J.M.M. 1995. *Traçados e limites da Ciência da Informação.* Ciência da Informação, Brasília, v.24, n.1, p.42-53, 1995.

PREECE, J.; SHNEIDERMAN, B. *The Reader-to-Leader Framework: Motivating Technology-Mediated Social Participation*. AIS Transactions on Human-Computer Interaction. 2009 v.1, n.1, p. 13-32

PREECE, J. J. I *Persuade, They Persuade, It Persuades!* Persuasive, LNCS 6137. Springer-Verlag Berlin Heidelberg. 2010. p.2-3.

RAPAILLE, C. *O código cultural: por que somos tão diferentes na forma de viver, comprar e amar?* Rio de Janeiro: Elsevier, 2007.

RENDÓN R., MIGUEL A.. *La ciencia de la información en el contexto de las ciencias sociales y humanas.* Ontología, epistemología, metodología e interdisciplina. *DataGramaZero - Revista de Ciência da Informação, v. 9, n. 4, ago. 2008. Disponível* em: <http://www.dgz.org.br>.

RICHARDSON, R. J. *Pesquisa social: métodos e técnicas.* São Paulo: Editora Atlas, 2007. 3ª Ed.

ROWLANDS, I. 1996. *Understanding Information Policy: Concepts, Frameworks and Research Tools.* Journal of Information Science 22, no. 1: 13-25.

SARACEVIC, T. *Ciência da informação: origem, evolução, relações.* Perspectivas em Ciência da Informação, Belo Horizonte, v.1, n.1, p.41-62, jan./jun. 1996.

SIANES, M. *Compartilhar ou proteger conhecimentos? Grande desafio no comportamento informacional das organizações*. In: Gestão Estratégica da Informação e Inteligência Competitiva. São Paulo: Saraiva, 2005.

SILVA, A., PINTO, J. *Uma visão global sobre as ciências sociais*. In A. Silva, J. Pinto: *Metodologia das ciências sociais* (11ª. Ed.; p. 17-18). Porto Alegre: Edições afrontamento. 2001.

SINGER, T; KIMBLES, S. L. The Cultural Complex. London: Brunner-Routledge, 2004.

SOLMS, R. V. *Information security governance*. South Africa, Springer, 2008.

SPINK, A.; COLE, C. *New Directions in Human Information Behavior*. Netherlands: Springer. 2006.

SUTTON, H. **Competitive intelligence.** In: Conference Board Research Report. n° 913. New York: The Conference Board, 1988.

SVEEN, F.O.; TORRES, J.M.; SARRIEGI, J.M. *Blind Information Security Strategy*. International Journal of Critical infrastructure Protection, v.2, 2009, p.95-109

TARAPANOFF, K. *Informação, conhecimento e inteligência em corporações: relações e complementaridade*. In: [organizadores] Tarapanoff, Kira. Inteligência, Informação e Conhecimento. Brasília: Instituto Brasileiro de Informação em Ciência e Tecnologia - IBICT. 2006. p.19-35

TERRY, N. P.; FRANCIS, L. P. *Ensuring the privacy and confidentiality of electronic health records.* University of Illinois Law Review. 2007. n.2, p.681-736.

VAN NIEKERK, J.F.; VON SOLMS, R. *Information Security Culture: A management perspective*. Computer & Security. 2010. n4.v.29, p.476.

_____. *A holistic framework for the fostering of an information security sub-*

culture in organizations. Information Security South Africa – South Africa Conference. South Africa. 2005. Disponível em: http://icsa.cs.up.ac.za/issa/2005/. Proceedings/Full/041_Article.pdf; 2006. Acesso em 25 dez. 2010.

VROOM, C. and R. von SOLMS (2004). *Towards information security behavioural compliance.* Computers and Security, 23(3), 191-198.

WACKS, R. Privacy: *A very short introduction*. New York: Oxford University, 2010.

WILSON, T. D. *A problemática da gestão do conhecimento.* In: [organizadores] Tarapanoff, Kira. *Inteligência, Informação e Conhecimento.* Brasília: Instituto Brasileiro de Informação em Ciência e Tecnologia - IBICT. 2006. p.37-55

WILSON, T. D. *Human Information Behavior.* Information Science Research. v. 3. n. 2. 2000.

WILSON, T. D. *Revisiting user studies and information needs.* Journal of Documentation, 2006, v. 62, p.680 – 684 (b)

WILSON, T. D. *On user studies and information needs*. Journal of Documentation, 2006, v. 62, p.658-670 (c)

WYLDER, J. *Strategic Information Security.* [s.l.]: Auerbach Publications, 2004.

WORKMANN. M. *Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security*. Wiley InterScience, 2007.
Análise de Dados Qualitativos: Estratégias Metodológicas para as Ciências da Saúde, Humanas e Sociais. São Paulo: Editora da Universidade de São Paulo, 2004. 3º edição.

YENISEY, M. M.; OZOK, A. A.; SALVENDY, G. Perceived security determinants in e-commerce among Turkish university students. In.: Behaviour & Information Technology, 24, 259–274. 2005.

9 - Anexos

ANEXO 1: Questionário Coleta de Dados

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
1	Qual seu sexo?	( )	( )	( )	( )
2	Qual é a sua escolaridade?	( )	( )	( )	( )
3	Você entende o que é segurança da informação	( )	( )	( )	( )
4	A segurança da informação na instituição na qual trabalho é responsabilidade apenas do setor de tecnologia da informação.	( )	( )	( )	( )
5	Você, dentro de suas atribuições e funções no dia-a-dia, se sente parte responsável pela segurança da informação praticada na instituição?	( )	( )	( )	( )
6	A partir das diretrizes que a instituição fornece sobre como agir seguramente, eu consigo entender como atuar e agir de modo a garantir a confidencialidade, disponibilidade e a integralidade dos dados com os quais trabalho.	( )	( )	( )	( )
7	Na minha percepção, a instituição investe mais em tecnologia para assegurar a segurança da informação corporativa e menos em treinamentos para as pessoas sobre segurança da informação e em políticas de segurança da informação.	( )	( )	( )	( )
8	Percebo que a instituição empreende e explora as ações de segurança da informação para, através delas, promover a melhoria continua dos processos institucionais.	( )	( )	( )	( )
9	Eu poderia dizer que as ações de segurança da informação em minha instituição geram conhecimento e promovem o aprendizado entre os colaboradores?	( )	( )	( )	( )
10	Frequentemente ocorrem interações sociais entre os colaboradores para discutir temas sobre segurança da informação.	( )	( )	( )	( )
11	Eu poderia dizer que a segurança da informação na instituição na qual trabalho faz parte do planejamento estratégico ou da gestão estratégica da empresa.	( )	( )	( )	( )
12	O desenvolvimento da segurança da informação na instituição na qual trabalho inclui proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo, sejam elas internas e/ou externas à organização.	( )	( )	( )	( )

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
13	Quando ocorre um incidente de segurança da informação na instituição, esse incidente é detectado, prevenido e documentado.	( )	( )	( )	( )
14	Estão claras as condutas que a instituição deseja que eu tenha com relação à segurança da informação? Como exemplo podemos citar a comunicação de incidentes de segurança.	( )	( )	( )	( )
15	Você fica ciente de todas as atualizações de avaliação de riscos de seu departamento, setor ou área?	( )	( )	( )	( )
16	Há ocorrência de auditorias sobre segurança da informação no seu departamento ou setor ou área?	( )	( )	( )	( )
17	Você sabe quem são as pessoas responsáveis pela segurança da informação na sua instituição?	( )	( )	( )	( )
18	Há instruções e políticas formais em sua instituição que ensinam como a empresa espera que você aja com relação à segurança da informação.	( )	( )	( )	( )
19	Há indicadores de segurança da informação que são avaliados pela instituição na qual trabalho.	( )	( )	( )	( )
20	Há indicadores de segurança da informação que são avaliados pelo setor / departamento no qual trabalho.	( )	( )	( )	( )
21	A instituição comunica aos colaboradores sobre os incidentes de segurança da informação ocorridos.	( )	( )	( )	( )
22	Conheço os procedimentos e políticas de segurança da informação adotadas pela instituição na qual trabalho.	( )	( )	( )	( )
23	Posso identificar as atuais medidas que estão sendo tomadas em relação à segurança informacional na instituição na qual trabalho.	( )	( )	( )	( )
24	Costumo conversar com colegas sobre incidentes de segurança da informação ocorridos comigo ou que tenham ocorrido com eles ou com alguém que conheçamos.	( )	( )	( )	( )
25	Tenho oportunidade de sugerir ações de segurança da informação na instituição na qual trabalho.	( )	( )	( )	( )
26	As especificações das políticas de segurança da informação da instituição na qual trabalho são de fácil compreensão.	( )	( )	( )	( )
27	Os riscos, ameaças e vulnerabilidades com relação à segurança da informação de minha organização são bem documentados.	( )	( )	( )	( )
28	Os riscos, ameaças e vulnerabilidades com relação à segurança das informações da organização na qual trabalho são devidamente comunicados aos colaboradores.	( )	( )	( )	( )

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
29	Analisando as políticas de informação da organização na qual trabalho, eu diria que elas são efetivas e suficientes para garantir a confidencialidade, integridade e disponibilidade das informações (principalmente das informações sigilosas).	( )	( )	( )	( )
30	Através das regras de segurança da informação disponibilizadas por minha organização, eu consigo entender qual deve ser o seu comportamento e como a empresa espera que eu aja com relação à segurança da informação.	( )	( )	( )	( )
31	Na minha instituição existem mecanismos de execução que propiciam o cumprimento das políticas de segurança da informação pelos colaboradores.	( )	( )	( )	( )
32	Eu sou orientado ou obrigado a fazer back-ups diários das informações por mim processadas em um servidor disponibilizado pela instituição.	( )	( )	( )	( )
33	Eu observo, ao utilizar o meu e-mail corporativo, que ocorre a supressão de mensagens que possuem anexos não solicitados.	( )	( )	( )	( )
34	A instituição permite que eu acesse a rede corporativa, grave dados em pen-drives, CD´s, DVD´s e/ou imprima informações para uso tanto no ambiente institucional quanto em casa.	( )	( )	( )	( )
35	Posso dizer que há envolvimento e apoio das gerências, diretorias e presidência no que concerne às ações se segurança da informação.	( )	( )	( )	( )
36	No ambiente corporativo eu tenho acesso irrestrito a todos os sites que precisar ou quiser consultar.	( )	( )	( )	( )
37	No ambiente institucional posso escolher quais itens das políticas de segurança da informação vou cumprir.	( )	( )	( )	( )
38	Altero mensalmente minhas senhas de acesso aos recursos corporativos (por exemplo: redes, computadores, mídias removíveis etc.).	( )	( )	( )	( )
39	Considero volumosa demais a quantidade de diretrizes, normas e procedimentos que devo cumprir.	( )	( )	( )	( )
40	Normalmente, acesso os sistemas de informação corporativos de minha casa (acesso remoto) para resolver algum problema ou atender a alguma demanda.	( )	( )	( )	( )
41	Posto em redes sociais fatos ou ocorrências que aconteceram na organização ou no meu setor para alertar amigos.	( )	( )	( )	( )

	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
42	Existe um check list de segurança da informação que devo seguir no meu dia-a-dia.	( )	( )	( )	( )
43	Sinto vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é segurança da informação de minha instituição.	( )	( )	( )	( )
44	Você poderia dizer que em primeiro lugar você dedica atenção à sua profissão e à especialidade do computador no qual trabalha para depois absorver os valores, missão e visão da empresa para a qual trabalha.	( )	( )	( )	( )
45	Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação propostas pela instituição.	( )	( )	( )	( )
46	Sou treinado para ter um comportamento seguro.	( )	( )	( )	( )
47	Sei com clareza qual é o meu papel na segurança informacional da empresa.	( )	( )	( )	( )
48	Existem, na instituição na qual trabalho, programas de educação para formar pessoas com relação à segurança da informação.	( )	( )	( )	( )
49	As ameaças de segurança da informação que sofro determinam meu comportamento frente às situações que vivencio.	( )	( )	( )	( )
50	Avaliando a situação atual, sinto que o ambiente da empresa é seguro no que concerne às informações que nele são processadas.	( )	( )	( )	( )
51	A alta carga de trabalho vinculada à minha atividade prejudica minha percepção e ação com relação à segurança da informação.	( )	( )	( )	( )

Anexo 2: Carta de apresentação do questionário

A Universidade Federal de Minas Gerais em parceria com a XXXXXXX conduzem pesquisa sobre segurança da informação no ambiente. Os pesquisadores responsáveis são Luciana Emirena dos Santos Carneiro e Dr. Maurício Barcellos Almeida.

Os colaboradores da diretoria de tecnologia serão os pioneiros a responder a pesquisa haja vista que nesse momento trabalharemos com vistas a ajudar na proteção das informações sensíveis à XXXXXXX. Essas informações são processadas em sua maior parte pela diretoria de tecnologia e por esse motivo você colaborador e suas opiniões são referência para este estudo.

As perguntas do questionário devem ser respondidas com base no que ocorre hoje dentro da instituição, ou seja, fatos antigos que não ocorrem mais ou ações futuras que ainda serão implementadas não devem ser considerados no ato da resposta.

Escolha apenas 1 resposta para cada questão.

Não é necessário se identificar. O anonimato é fator preponderante nessa pesquisa e você não corre risco de ser identificado.

As respostas aqui apresentadas serão processadas, manipuladas e armazenadas apenas pelos pesquisadores responsáveis com o máximo de sigilo. Garantimos a confidencialidade de todas as respostas! Pode confiar!

As questões a serem respondidas são todas fechadas, com quatro opções de respostas. No total serão 40 questões e o tempo de resposta total será de **no máximo** 20 minutos.

Suas respostas são muito importantes! Dedique um pouco do seu tempo e COLABORE! Este é um grande projeto e você muito provavelmente sentirá os frutos positivos dessa pesquisa expresso em ações no seu dia-a-dia. CONTAMOS COM VOCÊ!

Em caso de dúvidas, gentileza entrar em contato pelo e-mail:

segurancadainformacao2012@gmail.com

Muito Obrigado!