

Pedro Henrique de Moura Araujo

CONSTRUÇÃO DA ESCALA DO NÍVEL DA
CULTURA ORGANIZACIONAL DE SEGURANÇA DA
INFORMAÇÃO

Tese submetida ao
Programa de
Engenharia de Produção
da Universidade Federal
de Santa Catarina para a
obtenção do Grau de
Doutor em Engenharia
de Produção.

Orientador: Prof. Dalton
Francisco de Andrade,
PhD.

Florianópolis - SC
2018

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Moura Araujo, Pedro Henrique de
CONSTRUÇÃO DA ESCALA DO NÍVEL DA CULTURA
ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO / Pedro
Henrique de Moura Araujo ; orientador, Dalton
Francisco de Andrade Andrade, 2018.
205 p.

Tese (doutorado) - Universidade Federal de Santa
Catarina, , Programa de Pós-Graduação em Engenharia
de Produção, Florianópolis, 2018.

Inclui referências.

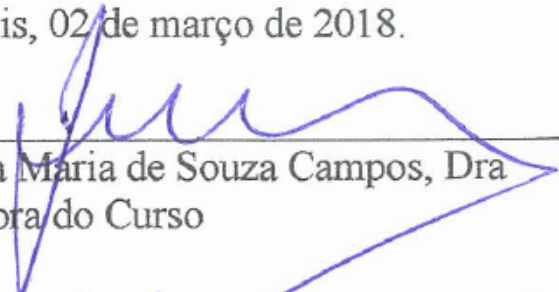
1. Engenharia de Produção. 2. Segurança da
Informação. 3. Cultura Organizacional. 4. Teoria da
Resposta ao Item. 5. Cadeia de Suprimentos. I.
Andrade, Dalton Francisco de Andrade . II.
Universidade Federal de Santa Catarina. Programa de
Pós-Graduação em Engenharia de Produção. III. Título.

Pedro Henrique de Moura Araujo

CONSTRUÇÃO DA ESCALA DO NÍVEL DA CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

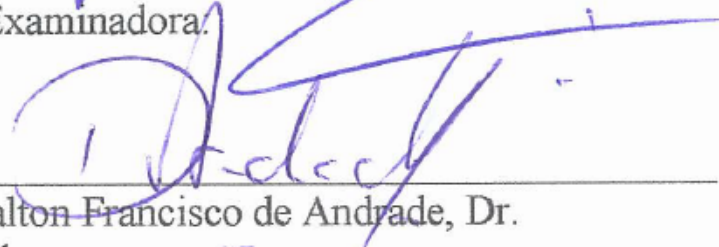
Esta Tese foi julgada adequada para obtenção do Título de “Doutor” e aprovada em sua forma final pelo Programa de Engenharia de Produção.

Florianópolis, 02 de março de 2018.

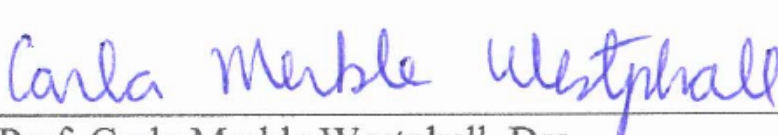


Prof.ª Lucila Maria de Souza Campos, Dra.
Coordenadora do Curso

Banca Examinadora.



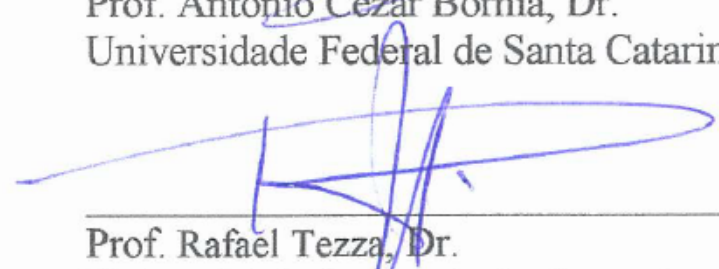
Prof. Dalton Francisco de Andrade, Dr.
Orientador
Universidade Federal de Santa Catarina



Prof. Carla Merkle Westphall, Dra.
Universidade Federal de Santa Catarina



Prof. Antonio Cezar Bornia, Dr.
Universidade Federal de Santa Catarina



Prof. Rafael Tezza, Dr.
Universidade do Estado de Santa Catarina

Este trabalho é dedicado à minha esposa e filhos que, ao longo dessa jornada, sempre estiveram do meu lado suprimindo de amor, dedicação e companheirismo. Aos meus pais e irmãos que entenderam o momento e me apoiaram na conquista do meu objetivo.

AGRADECIMENTOS

A Deus, por tornar tudo isso possível.

A minha esposa, meus filhos, minha filha e minhas noras, que são meu suporte emocional.

A minha mãe, meus irmãos e a Ana, por compreenderem esse momento e perdoarem as horas retiradas do convívio.

A minha grande família, de sangue e de escolha, pela inspiração e pelo exemplo. Aos meus sogros, um especial obrigado pelo apoio incondicional.

Ao meu orientador Prof. Dalton Francisco de Andrade pela disponibilidade, auxílio e, sobretudo, por acreditar em mim e permitir a concretização desse sonho.

Meu especial agradecimento ao Inep pela oportunidade de realização de um objetivo de vida: à Diretora-Presidente do Serpro, Sra. Maria da Glória Guimarães dos Santos, por ter apoiado essa pesquisa e colocado o Serpro à disposição; ao Dr. Jairo Schäfer, Diretor do Foro da Justiça Federal de Santa Catarina, por acreditar e ser o primeiro a participar da aplicação do questionário de coleta de dados; aos colegas da Universidade Católica de Brasília, prof. Ms. Fernando Gulart, prof. Ms. Vilson Hartmann e prof. Ms. Wesley Sepúlveda, por manter vivos a amizade e o coleguismo nos momentos de dificuldades.

Ao colega Jeovani Schmitt pelo companheirismo e pelas inúmeras ajudas com a estatística.

Aos colegas especialistas pela valiosa colaboração na construção desse trabalho:

Ms. Vilmondes Gomes da Silva

Mestre em Ciência em Informática-PUC/RJ

Professor de Engenharia de software, auditor líder, perito em qualidade em normas ISO.

Ms^a. Fabricia Lemos de Faria

Mestra em Ciência da Computação-UFSC

Analista no SERPRO

Ms. Ulysses Alves de Levy Machado

Mestre em propriedade intelectual (UFPE), Advogado, especialista em propriedade intelectual (GWU), especialista em segurança da informação - UnB, cátedra e orientação à pesquisa exercida em ambas (direito e segurança da informação), Coordenador Estratégico de Segurança da Informação - Serpro.

Ms. Marcos Allemand

Master's degree - Business Continuity - Norwich University

Especialidades: CISSP, CISM, CBCP, MCSO, BS7799 Lead Auditor, ITIL Foundation.

Analista de Sistemas no Serpro.

Aos professores Pedro Barbetta, Adriano Borgatto, Roberto Cruz por compartilhar seus conhecimentos comigo.

Aos mestres, colegas e funcionários da Universidade Federal de Santa Catarina que participaram dessa jornada.

“O que não pode ser medido, não pode ser gerenciado”

William Edwards Deming

RESUMO

O presente estudo objetivou a construção de uma escala de medida do nível de cultura organizacional de segurança da informação. Nesse sentido, a partir de uma ampla revisão bibliográfica, foi conceituada a cultura organizacional de segurança da informação, objeto de avaliação do estudo. Em seguida, procedeu-se a definição do traço latente – Cultura Organizacional de Segurança da Informação, estabelecendo que os atributos que caracterizam o traço latente são os nove princípios da Organização para Cooperação e Desenvolvimento Econômico – OCDE, e os controles de segurança da informação da norma ABNT NBR ISO/IEC 27002. Para a construção da escala, foi elaborado um instrumento de avaliação, questionário, e aplicado em organizações públicas federais. Após a análise e validação do instrumento, com fundamento na Teoria da Resposta ao Item – TRI obteve-se um conjunto de 55 itens que estruturam a escala. O estudo apresentou os seguintes resultados: a proposta de um conceito de cultura organizacional aplicada à segurança da informação e a criação de uma escala padronizada e interpretada de avaliação do nível de cultura organizacional de segurança da informação, definida em cinco níveis: 0 – Caos, 1 – Elementar, 2 – Em evolução, 3 – Encaminhado e 4 – Otimizado. A escala desenvolvida, fundamentada na TRI, permite avaliar todos os tipos de organizações, possibilita a comparabilidade entre organizações, inclusive aquelas pertencentes a uma cadeia de suprimentos, e fornece as informações necessárias para o autoconhecimento da organização, auxiliando os gestores na otimização dos investimentos em segurança da informação e nas tomadas de decisões gerenciais.

Palavras-chave: Segurança da Informação; Cultura Organizacional; Teoria da Resposta ao Item; Escala de Proficiência; Cadeia de Suprimentos.

ABSTRACT

The present study's goal was to build a measurement scale of the level of information security in an institution's organizational culture. Therefore, based on a broad bibliographical review, the study conceptualized the organizational culture of information security, which was our object of evaluation. Then, the study defined the latent trait – Organizational Culture of Information Security, establishing that the attributes that characterize the latent trait are: the nine principles of the Organization for Economic Cooperation and Development – OECD; and the information security controls of the ABNT NBR ISO / IEC 27002's standard. In order to build the scale, we developed an evaluation instrument, a questionnaire, and applied it to federal public organizations. After the analysis and validation of the instrument, based on Item Response Theory - IRT, we obtained a set of 55 items that structure the scale. The study yielded the following results: a proposal of a concept of organizational culture applied to information security; and the development of a standardized and interpreted scale of evaluation of the organizational culture level of information security, defined in five levels: 0 - Chaos, 1 - Elementary, 2 - In Progress 3 - Advanced and 4 - Optimized. The scale developed based on IRT allows us to evaluate all types of organizations, enables comparing organizations in a supply chain, and provides the necessary information for self-knowledge of the organization, helping managers to optimize investments in information security and in managerial decision-making.

Keywords: Information Security, Organizational Culture, Item Response Theory, Proficiency Scale, Supply Chain.

LISTA DE FIGURAS

Figura 1 - Níveis da Estrutura da Cultura Organizacional.....	46
Figura 2 - Processo de gestão de riscos de segurança da informação ...	63
Figura 3 - Relacionamento dos elementos da norma 27002	70
Figura 4 - Fluxo da metodologia.....	79
Figura 5 - Distribuição por categoria de resposta	98
Figura 6 - Curva de Informação do Instrumento	109
Figura 7 - Distribuição dos escores em cada nível nas organizações ..	127
Figura 8 - Curva Característica dos Itens - CCI.....	187

LISTA DE QUADROS

Quadro 1 - Matriz de Referência.....	83
Quadro 2 - Exemplo da constituição de um item.....	86
Quadro 3 - Composição dos blocos e cadernos	87
Quadro 4 - Limites de concentração por nível.....	125
Quadro 5 - Itens por Diretriz	149
Quadro 6 - Itens Recategorizados	179
Quadro 7 - Distribuição dos Itens por Nível de Proficiência.....	201
Quadro 8 - Posicionamento dos Itens na Régua de Proficiência	202
Quadro 9 - Análise Comparativa de Modelos de Maturidade da Segurança da Informação	203

LISTA DE TABELAS

Tabela 1 - Totalização da Coleta por Organização	97
Tabela 2 - Como você avalia o seu conhecimento sobre o tema?	98
Tabela 3 - Tempo gasto no preenchimento em minutos	99
Tabela 4 - Frequência de preenchimento	100
Tabela 5 - Frequência por caderno	100
Tabela 6 - Resultado final da análise fatorial de informação completa.....	104
Tabela 7 - Estimativas dos parâmetros dos itens na escala (0,1)	105
Tabela 8 - Frequência dos Itens por Níveis de Qualidade	107
Tabela 9 - Frequência por faceta	108
Tabela 10 - Parâmetros do teste	109
Tabela 11 - Posicionamento pela Média	124
Tabela 12 - Posicionamento pelo nível de concentração	126
Tabela 13 - Parâmetros após transformação	195
Tabela 14 - Frequência por escore	199

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CIT	Citigroup
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives For Information Related Technology
CEO	Diretor Executivo
CFI	Closefit
CFO	Diretor Financeiro
COO	Diretor de Operações
CIO	Diretor de Ti
CS	Cadeia de Suprimentos
CSI	Cultura de Segurança da Informação
CSIO	Diretor de Segurança da Informação
GISMM	Gartner's Information Security Awareness Maturity Model
GSMM	Generic Security Maturity Model
IBGE	Instituto Brasileiro de Geografia e Estatística
IBM	International Business Machines
IEC	International Engineering Consortium
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
INFOSEC	Information Security
ISACA	Information Systems Audit And Control Association
ISEM	Information Security Evaluation Maturity Model
ISF	Information Security Framework
ISI	Information Security Initiatives
ISM	Information Security Management
ISO	International Organization For Standardization
ITIL	Information Technology Infrastructure Library
MRG	Modelo de Resposta Gradual
NIST	National Institute of Standards and Technology
OCDE	Organismo de Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
PBIB	Blocos Incompletos Parcialmente Balanceados
RMSEA	<i>Root Mean Square Error of Approximation</i> Erro Quadrático Médio Aproximado
SI	Segurança da Informação
SOA	Service of Application
SSE	Systems Security Engineering
TCT	Teoria Clássica do Teste
TIC	Tecnologia de Informação e Comunicação
TLI	Tucker– Lewis Index
TRI	Teoria da Resposta ao Item

SUMÁRIO

1	INTRODUÇÃO	27
1.1	CONTEXTUALIZAÇÃO.....	27
1.2	PROBLEMA.....	29
1.3	OBJETIVOS	32
1.3.1	Objetivo Geral.....	32
1.3.2	Objetivos Específicos	32
1.4	JUSTIFICATIVA.....	32
1.4.1	RELEVÂNCIA E CONTRIBUIÇÃO.....	33
1.4.2	INEDITISMO.....	34
1.5	DELIMITAÇÕES	37
1.6	ESTRUTURA DA TESE.....	38
2	REFERENCIAL TEÓRICO	39
2.1	UM BREVE HISTÓRICO DA CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO.....	39
2.2	CULTURA.....	41
2.3	CULTURA ORGANIZACIONAL.....	43
2.3.1	Estrutura da Cultura Organizacional	45
2.4	SEGURANÇA DA INFORMAÇÃO	47
2.4.1	Segurança da Informação e Segurança Cibernética	51
2.4.2	Fator Humano	51
2.5	CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO.....	53
2.6	PRINCÍPIOS DIRETIVOS DE UMA CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO.....	57
2.6.1	Sensibilização (Consciência)	57
2.6.2	Responsabilidade.....	58
2.6.3	Resposta (Reação)	59
2.6.4	Ética.....	60
2.6.5	Democracia	61
2.6.6	Avaliação de risco.....	62
2.6.7	Projeto de segurança e implementação.....	65

2.6.8	Gestão de Segurança.....	66
2.6.9	Reavaliação.....	68
2.7	AVALIAÇÃO DA CULTURA.....	68
2.8	TEORIA PSICOMÉTRICA	72
2.8.1	Traço Latente	73
2.8.2	Validação	73
2.8.3	Fidedignidade	73
2.9	TEORIA DA RESPOSTA AO ITEM	74
3	MÉTODO.....	79
3.1	DELINEAMENTO DA PESQUISA.....	79
3.2	DELINEAMENTO TEÓRICO	80
3.3	DEFINIÇÃO DO TRAÇO LATENTE	81
3.4	ELABORAÇÃO DOS ITENS.....	81
3.5	CONSTRUÇÃO DO INSTRUMENTO DE COLETA	86
3.6	COLETA DE DADOS.....	88
3.7	PROCEDIMENTOS PARA ANÁLISE DO INSTRUMENTO	89
3.7.1	Consistência dos cadernos.....	90
3.7.2	Consistência dos itens	90
3.7.3	Dimensionalidade do Instrumento	90
3.7.4	Independência local	91
3.7.5	Avaliação da qualidade dos itens	92
3.7.6	Calibração dos itens.....	92
3.8	VALIDAÇÃO DO MODELO.....	93
3.9	VALIDAÇÃO DE CRITÉRIO.....	93
3.10	CONSTRUÇÃO DA ESCALA.....	94
4	ANÁLISE DOS RESULTADOS E DISCUSSÃO.....	97
4.1	COLETA DE DADOS.....	97
4.2	ANÁLISE DO INSTRUMENTO.....	99
4.2.1	Análise de consistência dos cadernos.....	99
4.2.2	Análise de consistência dos itens	101
4.2.3	Agrupamento das categorias dos itens	102
4.2.4	Dimensionalidade do Instrumento	102
4.2.5	Calibração dos itens.....	105

4.3	VALIDAÇÃO DO MODELO	109
4.4	VALIDAÇÃO DE CRITÉRIO	110
4.5	CONSTRUÇÃO E INTERPRETAÇÃO DA ESCALA	110
4.5.1	Interpretação da escala.....	111
4.5.2	Posicionamento da organização.....	123
4.6	SÍNTESE DO CAPÍTULO	127
5	CONCLUSÃO E SUGESTÕES PARA TRABALHOS	
	FUTUROS	129
5.1	CONCLUSÃO	129
5.2	SUGESTÕES PARA TRABALHOS FUTUROS.....	131
	REFERÊNCIAS	133
	APÊNDICE A – Itens por Diretriz.....	149
	APÊNDICE B – Itens Recategorizados.....	179
	APÊNDICE C – Gráfico dos itens	187
	APÊNDICE D – Parâmetros Transformados	195
	APÊNDICE E – Frequência por escore	199
	APÊNDICE F – Itens / proficiência.....	201
	APÊNDICE G – Quadro Comparativo de Metodologias de	
	Maturidade.....	203

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

A globalização conectou a humanidade. Na atual sociedade da informação, a todo instante, as pessoas são surpreendidas com notícias de quebras de segurança, violações e/ou uso inadequado das informações que corrompem sistemas, expõem usuários e empresas, danificam protocolos, fraudam dados, podendo, inclusive, incorrer em decisões equivocadas e medidas prejudiciais à política, à economia e à soberania dos países.

Cabe ressaltar o escândalo originado pelo caso Edward Snowden, da Agencia Nacional de Segurança dos Estados Unidos da América – NSA/EUA, que expôs, ao conhecimento de todos os cidadãos, o mundo da espionagem eletrônica entre nações soberanas e independentes, e demonstrou, principalmente, o quanto as organizações e a sociedade se mostram vulneráveis quando o quesito é segurança da informação.

Com respeito à informação enquanto valor organizacional é importante referenciar a pesquisa sobre o estado da informação (*State of Information*) realizada em 2012 e publicada em 17 de junho de 2012 pela empresa Symantec, uma das líderes mundiais em segurança da informação. A pesquisa revelou que a informação custa às empresas em todo o mundo cerca de US\$ 1,1 trilhão por ano. São essas informações digitais que garantem às empresas eficiência, competitividade e permanência no mercado. Assim, concluiu a pesquisa que, em 2012, o acervo de informações digitais representava 49% do valor total de mercado de uma organização (SYMANTEC, 2012). É de supor que, com o crescimento do uso da tecnologia, o valor da informação digital para a empresa aumente, significativamente, a cada ano.

Por outro lado, de acordo com os estudos conduzidos pelo *Ponemon Institute*, sediado em Michigan – EUA, instituição especializada em proteção de dados e segurança da informação, o custo médio por registro violado/comprometido, em 2016, aumentou de US\$ 154 para US\$ 158 e o custo total médio da violação de dados aumentou de US\$ 3,8 para US\$ 4 milhões. O estudo abrangeu 383 empresas em 16 setores da indústria nos seguintes países: Estados Unidos, Reino Unido, Alemanha, Austrália, França, Brasil, Japão, Itália, Índia, Região árabe, Canadá e África do Sul. Os registros violados/comprometidos totalizaram, entre as organizações pesquisadas, de 3.000 a 101.500 (PONEMON INSTITUTE, 2016).

No relatório de 2017 a IBM constatou que aproximadamente 47% das organizações pesquisadas apontaram que os incidentes foram causados por ataques maliciosos ou criminosos e que o custo médio por registro violado/comprometido foi de US\$ 156,00. Embora os ataques maliciosos sejam os mais caros, o custo médio dos incidentes por falha no sistema e erro humano foi de US\$ 128,00 e US\$ 126,00, respectivamente, sugerindo, portando, que o fator humano (negligência) pode ser tão oneroso quanto as falhas no sistema. Outro achado relevante da pesquisa foi que 31% de todas as violações foram causadas por negligência dos funcionários e 25% foram causadas por falhas no sistema (PONEMON INSTITUTE E IBM SECURITY, 2017).

Nesse sentido, um estudo mundial realizado pela PwC, em parceria com as revistas CIO e CSO que consistiu em uma enquete, por meio da Internet, junto a 9600 executivos de 115 países, concluiu que os funcionários e ex-funcionários representam 57% aos incidentes de origem interna e que os *Hackers* respondem por 32% dos ataques externos (PWC, 2014).

Essa estatística vem corroborar com a literatura, ao confirmar que a maioria das violações da segurança da informação são causadas por falhas humanas associadas à inconsciência ou ingenuidade. O fator humano na segurança da informação vem sendo reconhecido, pelos pesquisadores, como sendo o ponto mais importante nas ameaças à segurança da informação (PARSONS, MCCORMAC *et al.*, 2014; PARSONS, YOUNG *et al.*, 2015).

Diante de dados que se revelam tão expressivos envolvendo o custo da informação para a organização e o custo da violação dessa informação, o gerenciamento da segurança da informação tem desempenhado um papel de destaque nas discussões empreendidas pela governança corporativa, pois representa o impulsionador de melhoria do negócio (SINDHUJA, 2014).

As questões que envolvem a segurança da informação e as práticas de segurança também precisam ser examinadas na cadeia de suprimentos – CS, a partir de perspectivas internas e externas, ou intra e inter-organizacional (DHILLON, 2007; NADLER E KROS, 2008), uma vez que as organizações pertencentes a uma CS têm optado pela utilização da Internet como meio rápido e eficiente de troca de informações, porém, como se sabe, menos seguro que as conexões privadas particulares. Assim, uma violação ou um ataque à segurança de uma das organizações pode expor todas as demais organizações da CS (BANDYOPADHYAY, JACOB *et al.*, 2010), comprometendo o mais

importante ativo que são as informações trocadas entre parceiros comerciais (SINDHUJA, 2014), ou até mesmo, o fornecimento do produto da CS.

O que se verifica na literatura é que as questões técnico-operacionais têm sido abordadas de forma mais proeminente para minimizar as falhas na segurança da informação. No entanto, pouca atenção é dada ao papel dos fatores humanos nas organizações, mas os estudos demonstram que esses fatores são indispensáveis para garantir a salvaguarda das informações organizacionais. Para tanto, é fundamental entender o comportamento individual e coletivo, suas atitudes sobre segurança da informação e a relação desses fatores com a cultura organizacional (VROOM E VON SOLMS, 2004; ALFAWAZ, NELSON *et al.*, 2010).

O desafio das organizações reside, portanto, em incutir uma segurança comportamental, ou seja, a implementação de uma cultura organizacional de segurança da informação (DHILLON, TEJAY *et al.*, 2007; ALFAWAZ, NELSON *et al.*, 2010).

1.2 PROBLEMA

A informação carrega consigo um valor agregado. Logo, é possível afirmar que os dados e as informações de uma instituição integram seu patrimônio intangível, configurando-se em verdadeiros ativos. A ABNT adota, na NBR ISO/IEC 13335-1:2004, a seguinte definição de ativo: “qualquer coisa que tem valor para a organização” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a, p. 2).

Portanto, sendo a informação um recurso ou matéria prima, possui um valor estimável para as organizações. Nesse sentido, a norma NBR ISO/IEC 27002:2013 estabelece que “Informação, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b, p. x).

O ministro Walter Rodrigues do Tribunal de Contas da União, órgão máximo de fiscalização dos gastos públicos, sintetiza bem a preocupação institucional com a segurança da informação quando diz:

Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança da informação tornou-se um ponto crucial para a sobrevivência das insti-

tuições. (TRIBUNAL DE CONTAS DA UNIÃO, 2007).

A Segurança da Informação é uma área do conhecimento complexa que envolve várias subáreas, cada uma com um perfil específico, o que possibilita uma diversidade de definições disponíveis sobre o tema.

A norma NBR ISO/IEC 17799:2005 propõe uma definição sintetizada de segurança da informação para as organizações como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. ix).

Logo, a segurança da informação é, para as organizações, um requisito de negócio, a garantia de permanência no mercado, pois objetiva proteger o investimento realizado pela organização nas informações, ou seja, em seus ativos, em seu patrimônio (RASHID, ZAKARIA *et al.*, 2013), e aperfeiçoar a colaboração e a coordenação entre as organizações pertencentes à CS (BANDYOPADHYAY, JACOB *et al.*, 2010).

Considerando que as pessoas representam o elo mais fraco do processo de gerenciamento da segurança da informação nas organizações, é necessário o envolvimento dos colaboradores no estabelecimento de uma cultura organizacional de segurança da informação para que possa haver um alinhamento da cultura “prévia”, aquela que os indivíduos carregam consigo, com os valores da organização (VROOM e VON SOLMS, 2004; ALFAWAZ, NELSON *et al.*, 2010; PARSONS, YOUNG *et al.*, 2015).

Uma definição clara, por parte da organização, dos procedimentos de controle dos riscos e das responsabilidades de segurança incentivam os colaboradores a adotarem comportamentos éticos adequados e a cumprirem as orientações organizacionais, permitindo, assim, uma maior garantia de sucesso de segurança na rede de informações (MARTINS e ELOFF, 2002; DOJKOVSKI, LICHTENSTEIN *et al.*, 2010).

Mas, como implementar uma política organizacional de segurança da informação sem conhecer a cultura da organização? Essa cultura, que é composta das práticas de segurança da informação incorporadas no ambiente de trabalho da organização, precisa ser medida para ser conhecida (MARTINS e ELOFF, 2002).

A mensuração da cultura organizacional pré-existente desempenha um papel importante para auxiliar a organização a entender sua própria cultura e subsidiar a tomada de decisão estratégica para adoção

de medidas de melhorias visando alcançar a cultura de segurança da informação desejada (OKERE, VAN NIEKERK *et al.*, 2012)

No entanto, não existe uma definição aceita e prática de cultura organizacional de segurança da informação (MALCOLMSON, 2009). Logo, não existe uma maneira de medir a cultura de segurança que possa ser usada, de forma objetiva, para comparar a cultura entre organizações com objetivos comerciais e domínios diferentes.

Verifica-se que os procedimentos de medida do nível da cultura organizacional de segurança da informação ainda não se apresentam de forma uniforme ou padronizada. Conforme sustentam Breier e Hudec (2012, p. 1) “As abordagens de avaliação de risco na tecnologia da informação são, principalmente, baseadas em métodos subjetivos e qualitativos de medição e avaliação”.

O gerenciamento da segurança da informação tão pouco se mostra uma entidade quantificável e sua avaliação é complexa, haja vista a perspectiva eletrônica associada (ELOFF e VON SOLMS, 2000).

Assim, a questão de pesquisa a ser atendida é: Como medir o nível da cultura organizacional de segurança da informação?

Considerando que cada organização forma sua própria cultura e que não há uma prática comum (MALCOLMSON, 2009), faz-se necessária a utilização de padrões que sejam aceitos entre as organizações para que o instrumento de medida possa aferir o nível de cultura organizacional de segurança da informação de forma objetiva, permitindo a análise e a comparação dos resultados.

A proposta dessa pesquisa, para o atendimento do problema posto, é desenvolver um modelo de medida do nível da cultura organizacional de segurança da informação, em função das diretrizes sobre cultura organizacional de segurança da informação estabelecidas pela Organização de Cooperação e Desenvolvimento Econômico - OCDE e dos requisitos técnicos das normas regulamentadoras da família ABNT NBR ISO/IEC 27000, por meio da utilização da Teoria da Resposta ao Item – TRI, eficiente metodologia de avaliação quantitativa de variáveis que não podem ser medidas diretamente (BORTOLOTTI, 2010).

Define-se TRI como "um conjunto de modelos matemáticos que procuram representar a probabilidade de um indivíduo dar uma certa resposta a um item como função dos parâmetros do item e da habilidade (ou habilidades) do respondente." (ANDRADE, TAVARES *et al.*, 2000, p. 7). No presente estudo, esse conjunto de modelos matemáticos (TRI) busca representar a probabilidade do colaborador escolher a opção em função da sua habilidade em segurança da informação.

Por meio da TRI é possível estabelecer qualquer medição a partir de um conjunto de características do objeto de estudo que se pretende mensurar (VARGAS, 2007). A esse objeto de estudo dá-se o nome de traço latente, que, para a pesquisa, é a cultura organizacional de segurança da informação.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Construir uma escala de medida do nível da cultura de segurança da informação nas organizações, utilizando a Teoria da Resposta ao Item.

1.3.2 Objetivos Específicos

- Conceituar o traço latente: cultura organizacional de segurança da informação;
- Elaborar o instrumento de avaliação; e
- Criar a escala de medida da cultura organizacional de segurança da informação.

1.4 JUSTIFICATIVA

A maior dificuldade enfrentada na avaliação da cultura organizacional de segurança da informação, conforme já relatado, reside, justamente, na falta de uma medida quantitativa, objetiva e aceita (MALCOLMSON, 2009), que leve em consideração os fatores subjetivos que influenciam ou se relacionam no gerenciamento da segurança da informação e que não podem ser avaliados de forma direta. Uma vez que nem todo elemento que compõe a medida pode ser avaliado diretamente, a avaliação tende a assumir um viés de infraestrutura (ELOFF E VON SOLMS, 2000).

Nesse sentido, em busca de metodologias quantitativas para se avaliar a segurança de informação, foram desenvolvidas algumas metodologias (*frameworks*) para mensurar a maturidade da organização em segurança da informação, por meio de seus processos, tais como COBIT, ISM3, ISF-IBM, CMMI, dentre outros. No entanto, todos apresentam deficiências no que tange aos fatores humanos, comportamentais e culturais (vide Apêndice G - Quadro Comparativo de Metodologias de Maturidade).

Uma vez que o objeto de avaliação proposto, cultura organizacional de segurança da informação, não pode ser mensurado de forma direta, necessita-se de uma metodologia capaz de atribuir uma medida que

represente o seu valor. A TRI, fundamentada na psicometria, teoria da medida em ciências para explicar aspectos psicológicos (PASQUALI, 1997), permitirá a quantificação das variáveis que compõem o traço latente - cultura organizacional de segurança da informação.

Ademais, como a TRI se preocupa em construir itens válidos para avaliar os elementos do traço latente, as vantagens na sua utilização são: a produção de itens de qualidade que possibilitam a realização de tantos testes válidos quanto os itens permitirem (PASQUALI, 1997); a possibilidade de inclusão de novos itens, desde que estejam na mesma unidade de medida (KOLEN E BRENNAN, 2014); e, sobretudo, a comparação da avaliação da cultura organizacional de segurança da informação entre organizações diferentes, inclusive entre as organizações pertencentes a uma cadeia de suprimentos, já que a TRI enfoca os itens e não o questionário como um todo (ANDRADE, TAVARES *et al.*, 2000).

1.4.1 RELEVÂNCIA E CONTRIBUIÇÃO

A relevância da pesquisa consiste no fato de que existe uma lacuna metodológica para a determinação quantitativa do nível da cultura organizacional de segurança da informação. O estudo mostra que a metodologia desenvolvida permitirá aos técnicos, gestores e pesquisadores avaliar o nível da cultura organizacional de segurança da informação com maior precisão, pois será possível quantificá-la e, consequentemente, criar uma escala interpretada que reflete de modo qualitativo os resultados quantitativos.

A escala, portanto, subsidiará o gestor na compreensão do comportamento dos seus colaboradores, da cultura e dos padrões existentes, dos pontos fortes e fracos do gerenciamento da segurança da informação, bem como possibilitará o acompanhamento longitudinal da evolução cultural da organização ao longo do tempo e a comparação com outras organizações, características inerentes à TRI (ANDRADE, TAVARES *et al.*, 2000).

A utilização da escala contribuirá na avaliação da eficácia, eficiência e efetividade do investimento realizado pelas organizações (RASHID, ZAKARIA *et al.*, 2013), da homogeneidade do nível de segurança nas organizações pertencentes a uma cadeia de suprimentos (DHILLON, 2007; NADLER e KROS, 2008), e subsidiará a alta administração nas decisões estratégicas para o aprimoramento necessário da segurança da informação.

1.4.2 INEDITISMO

Para a fundamentação do trabalho, realizou-se uma pesquisa bibliográfica em diversas bases de publicações. O procedimento de pesquisa processou-se, principalmente, por meio de busca a partir do sítio da Capes, no endereço <http://www-periodicos-capes-gov-br>, utilizando a conexão VPN da UFSC. A decisão pelo caminho escolhido deve-se ao fato de que se trata de um portal com acesso simultâneo a várias bases de dados de publicações de trabalhos e pesquisas científicas, tais como: IEEE, Scopus, SciElo, Web of Science e EBESCO.

A busca pautou-se nas palavras-chaves, previamente selecionadas e adicionadas ao longo do levantamento realizado, que se verificaram mais frequentes nas publicações relacionadas à área, objeto do estudo. Em prosseguimento, foram adotados os critérios de "qualquer ano", "todos os tipos de materiais" e "qualquer idioma".

Denota-se, na tabela 1 abaixo, a síntese do trabalho de levantamento, bem como a demonstração da frequência de publicações de artigos científicos pertinentes, verificada em dois momentos distintos. No primeiro, a pesquisa foi realizada objetivando a ocorrência das palavras-chaves livre de qualquer restrição. No segundo momento, assumiu-se a restrição de exatidão na conformidade com o texto posto.

Tabela1 – Frequência da Ocorrência das Principais Palavras-chaves Aferidas nas Bases de Dados Disponíveis

Palavras-chave	Sem Restrição			Texto Exato		
	Qualquer	No Título	No Assunto	Qualquer	No Título	No Assunto
Total	3.523.662	387.298	98.249	256.872	36.579	69.212
Information security	524.457	64.688	16.792	25.868	5.561	2.487
Information security culture	101.629	567	55	53	10	11
information systems security	280.715	20.325	4.793	2.060	168	191
Information security awareness	73.907	1.183	115	248	45	28
Information security topics	61.286	623	14	35	0	2
Information security trends	98.526	2.148	711	13	1	3
Information activity	2.854	21	27	2.854	21	27
Information security responsibility	31	1	1	31	1	1
Information security human	201.810	3.270	212	17	0	2
Information Security Human Factors	112.896	442	21	3	0	2
Information Security Violation	27.800	208	14	1	0	0
Information Security Measure	157.905	1.528	44	18	0	0
Information Security Risk	190.520	4.529	557	461	54	70

Information Security Risk Assessment	76.250	841	117	82	16	19
Information Security Risk Analysis	138.756	1.524	119	58	5	22
Human Values Theory	32	5	0	0	0	0
Human Attitude	245.221	8.585	730	354	5	1
Risk Assessment	1.189.940	276.120	73.886	224.332	30.690	66.338
Security Violation	39.127	690	41	384	2	8

Fonte: Próprio autor

Da revisão da literatura relacionada ao tema Cultura Organizacional de Segurança da Informação, é possível constatar o ineditismo do trabalho nos seguintes aspectos:

1. A apresentação, pelo próprio autor, de conceito de cultura organizacional de segurança da informação;
2. A inclusão, no instrumento de medida, dos fatores humanos na avaliação da segurança da informação;
3. A adoção da TRI como metodologia para o desenvolvimento de uma escala de medida quantitativa da cultura em segurança da informação;
4. A adoção, em conjunto, de dois padrões internacionalmente aceitos, fundamentados nas diretrizes sobre cultura organizacional de segurança da informação estabelecidas pela OCDE (2002) e nas normas da ANBT ISO/IEC 27000 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a), para a construção dos itens do instrumento de avaliação; e
5. A construção de uma escala de medida da cultura organizacional de segurança da informação que permite a avaliação e a comparação entre organizações, ao longo do tempo.

Destaca-se, portanto, além da relevância da pesquisa e das contribuições que se pretende apresentar, o ineditismo do trabalho para o meio acadêmico e sua significativa utilidade para as organizações corporativas.

1.5 DELIMITAÇÕES

O objetivo do trabalho de pesquisa é a construção de uma escala de medida do nível de cultura de segurança da informação nas organizações, com a utilização da TRI, desenvolvida em função das diretrizes sobre cultura organizacional de segurança da informação estabelecidas pela OCDE (2002) e dos requisitos técnicos definidos nas normas da ANBT ISO/IEC 27000 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a), por representarem padrões internacionalmente aceitos. Esses dois padrões fundamentam a definição da matriz de descritores dos itens do instrumento de avaliação (vide Quadro 1 - Matriz de Referência).

Para a construção da escala foram coletados os dados juntos aos colaboradores de organizações selecionadas, independentemente do seu tipo, tamanho e finalidade.

1.6 ESTRUTURA DA TESE

A pesquisa aqui descrita está estruturada em cinco capítulos, descritos a seguir.

O Capítulo 1 – Introdução: apresenta a contextualização do problema, a questão de pesquisa, os objetivos (geral e específicos), as justificativas que subsidiaram a escolha do tema, a relevância e contribuição, o ineditismo e as delimitações do estudo.

O Capítulo 2 - Referencial Teórico: apresenta os fundamentos e as bases na literatura que servem para respaldar a pesquisa, nos seguintes temas: Histórico da Segurança da informação, Cultura, Cultura Organizacional, Segurança da Informação, Princípios Diretivos da OCDE e as normas da família ABNT NBR ISO/IEC 27000, e Teoria da Resposta ao Item.

O Capítulo 3 Método: apresenta todos os métodos utilizados no desenvolvimento da pesquisa, suas justificativas e as fundamentações teóricas.

O Capítulo 4 Análise dos resultados e Discussão: apresenta uma análise e discussão dos resultados alcançados durante a execução da pesquisa: análise dos itens e sua consistência, a necessidade de recodificação dos itens, análise da dimensionalidade do instrumento, teste de independência local, calibração dos itens, as validações do modelo e de critério e a construção e interpretação da escala da cultura organizacional de segurança da informação.

O capítulo 5 Conclusão e Sugestões de Trabalhos Futuros: apresenta as considerações finais sobre o resultado da pesquisa e apresentação de sugestões para estudos complementares.

2 REFERENCIAL TEÓRICO

Este capítulo dedica-se a apresentar os resultados obtidos a partir dos estudos sobre conceituação, fundamentos e abrangência da cultura organizacional de segurança da informação.

As empresas atuais operam em um ambiente interconectado e global que lhes permite colaborar entre si e compartilhar recursos de informação. Ao mesmo tempo, essa interconectividade expõe a organização a muitas ameaças internas, citando seus colaboradores, e externas. A ameaça interna está entre os principais problemas de segurança da informação que as organizações enfrentam, pois o fator humano é considerado o elo mais fraco da cadeia de segurança. Sabe-se que o homem traz consigo o seu padrão de comportamento associado a uma cultura. Criar ou modificar uma cultura de segurança é reforçar e aprimorar os mecanismos de proteção à informação. Surgem, assim, os estudos sobre cultura de segurança da informação (RASHID, ZAKARIA *et al.*, 2013).

Como já relatado, toda organização gera informação para, a partir dela, os gestores tomarem as decisões estratégicas. Essas informações compõem, portanto, o ativo da organização e, assim, têm valor e necessitam ser protegidas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b, p. x). Logo, as organizações necessitam investir em um processo crescente de aculturação em segurança da informação.

Inicialmente, cabe relatar, de forma sucinta, o panorama da evolução da cultura de segurança da informação nas organizações.

2.1 UM BREVE HISTÓRICO DA CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

O pesquisador Von Solms (2000; 2006) elaborou um estudo que apresenta a evolução da cultura de segurança da informação ao longo do tempo. Ele observou que a cultura de segurança da informação passou por quatro períodos os quais ele chamou de ondas.

A primeira onda chamada de Onda Técnica ocorre no início dos anos de 1980, período em que a computação era centralizada em *Mainframe* e teve como premissa que o problema da

segurança da informação era exclusivamente técnico. Nesse período as organizações fizeram investimentos em softwares, criptografias, dispositivos de autenticação e serviços de controle de acesso (VON SOLMS, 2000; KARLSSON, ASTRÖM *et al.*, 2015).

No entanto, só a adoção de soluções técnicas para a proteção da informação não foram suficientes, nem tampouco eficientes uma vez que os controles e as implementações de soluções continuavam dependentes da competência e da confiabilidade das pessoas envolvidas no processo (DHILLON, 2001; MARTINS e ELOFF, 2002).

A segunda onda é a do Gerenciamento, entre as décadas de 80 e 90. Neste período ocorrem os movimentos de *downsizing*, da computação distribuída e da Internet, a WWW e o comércio eletrônico. Essa evolução tecnológica permitiu a criação de uma especialidade técnica em segurança da informação. As organizações perceberam a necessidade da intervenção da alta administração no processo da segurança da informação, o que levou a adoção de políticas, procedimentos e métodos de segurança da informação, bem como a contratação de técnicos de segurança. Ainda na segunda onda as organizações perceberam que a dimensão humana da segurança da informação talvez fosse o maior problema (VON SOLMS, 2000; RAISCH, 2014).

A terceira onda ficou conhecida como a onda da Institucionalização. Ocorreu no final da década de 90 e teve como principal contribuição o início do desenvolvimento do conceito de cultura organizacional de segurança da informação. O objetivo era fazer com que a segurança da informação se tornasse uma atividade cotidiana para os funcionários da organização. É o período no qual as organizações também passaram a se preocupar com padronizações, certificação internacional e métricas (VON SOLMS, 2000; KRAEMER e CARAYON, 2005).

A quarta onda é a da Governança de Segurança da Informação. A governança foi definida pelo instituto *It Governance Institute* (2006, p. 11, tradução do autor) como sendo:

Um conjunto de responsabilidades e práticas exercidas pela alta administração com o objetivo de fornecer orientação estratégica, garantindo que os objetivos sejam alcançados, determinando que os riscos se-

jam gerenciados adequadamente e verificando que os recursos da empresa são usados de forma responsável.

Assim, a quarta onda trouxe uma evolução do conceito de gestão da informação, pois a governança é mais abrangente, tendo a gestão da segurança da informação como um dos processos da governança. Essa onda é caracterizada pela definição do papel da alta administração na organização, dada a importância e relevância no tratamento da questão (VON SOLMS, 2006).

A preocupação com a segurança da informação e a segurança cibernética, em um contexto de política internacional mundial, levou a Organização das Nações Unidas - ONU a publicar a Resolução 58/199 de 30/01/2004 - Criação de uma Cultura Global de Segurança Cibernética e Proteção Crítica da Infraestrutura da Informação, por meio da qual convoca as nações a se preocuparem com o tema de forma padronizada. Em 2010, a ONU amplia a norma anterior pela Resolução 64/211 - Criação de uma Cultura Global de Segurança Cibernética e Levantamento dos Esforços Nacionais para Proteger Infraestruturas Críticas de Informação (ONU, 2004; 2010; ASTAKHOVA, 2014).

A questão da segurança da informação e da segurança cibernética é um movimento que pertence a todos os países, a todas as organizações e a todas as pessoas. Trata-se de um movimento que estabelece novos paradigmas a todo momento.

Assim, torna-se imprescindível a apresentação de uma revisão teórica dos conceitos abrangidos pelo tema, quais sejam: cultura, cultura organizacional e segurança da informação no contexto das organizações para, então, buscar consolidar uma definição de cultura organizacional de segurança da informação, objeto de avaliação do estudo.

2.2 CULTURA

O conceito e definição de cultura vêm da antropologia. Conforme historia o antropólogo Laraia (2001), por volta do final do século XVIII e no princípio do seguinte, utilizavam-se dois termos para abordar o tema que hoje se entende como cultura. *Kultur* era o termo germânico para simbolizar todos os aspectos espirituais de uma comunidade, enquanto que a palavra francesa *Civilization* fazia referencia às realizações materiais de um povo. Em seu livro, Laraia (2001) relata que o britânico Edward B

Tylor (1832-1917) sintetizou os dois conceitos e criou o termo inglês *Culture*, que vem sendo utilizado desde então. Cita-se, abaixo, a definição de Laraia (2001, p. 25):

Tomado em seu amplo sentido etnográfico é este todo complexo que inclui conhecimentos, crenças, arte, moral, leis, costumes ou qualquer outra capacidade ou hábitos adquiridos pelo homem como membro de uma sociedade.

Hofstede (1993) ensina que a cultura "é a programação coletiva da mente que distingue um grupo ou categoria de pessoas de outro". Essa programação reflete em comportamentos individuais e coletivos observáveis ou mensuráveis, verbais e não verbais.

Em geral verifica-se que as definições de cultura são aplicadas a um subconjunto da sociedade. Os pesquisadores em segurança da informação Luo, Warkentin *et al.* (2009, p. 2, tradução do autor) definiram cultura como "um sistema de significado coletivo do grupo humano e é composto por seus valores, atitudes, crenças, padrões de idioma, costumes e pensamentos".

Para Malcolmson (2009) a cultura pode ser um conjunto de entendimentos comuns, padrões, valores e crenças que interagem com a estrutura de uma organização e é expresso por meio de uma linguagem que produz as normas comportamentais.

A descrição e a definição de cultura divergem entre os pesquisadores devido ao fato de que a cultura é multifacetada. No entanto, embora as definições de cultura sejam diferentes, elas convergem para o consenso de que a cultura inclui um conjunto comum de entendimentos (crenças) que são compartilhados pelos membros de um grupo social específico (MALCOLMSON, 2009).

Não obstante, independente do grupo social ou do objeto de observação, de alguma forma as definições dos estudiosos manifestam os elementos culturais já abordados por Laraia (2001, p. 45) "a cultura é um processo acumulativo, resultante de toda a experiência histórica das gerações anteriores. Este processo limita ou estimula a ação criativa do indivíduo".

Ora, se a cultura é um processo em constante evolução/modificação e é responsável pelas atitudes, valores e crenças do homem pertencente a um grupo social, é indispensável que a

organização, dependente do comportamento de seus colaboradores para obtenção de resultados, reconheça a importância do estabelecimento de uma cultura organizacional coerente com os valores e a política da empresa.

Nesse sentido, Martins e Eloff (2002) reforçam a importância de a administração formar o comportamento que pretende que seja a referência para seus colaboradores, para, com o tempo, desenvolver uma cultura própria da organização.

2.3 CULTURA ORGANIZACIONAL

Ao compreender o conceito de cultura, pode-se perceber o quanto importante é para uma organização a definição de seus valores e o estabelecimento de normas de comportamento individual que formarão o alicerce da cultura organizacional (DEAL E KENNEDY, 1982; LEIDNER E KAYWORTH, 2006).

Os estudos sobre a cultura da organização datam do início do século com a experiência de Hawthorne entre 1927 e 1932 (FERNANDES E ZANELLI, 2006). Ao longo do tempo os pesquisadores vêm evoluindo o conceito de cultura organizacional. Essa constante evolução faz com que exista uma falta de consenso quanto à definição e composição da cultura organizacional na literatura (PARSONS, YOUNG *et al.*, 2015).

Segundo Bali (1999) o conceito de cultura organizacional vem de princípios adotados na antropologia, objetivando a fundamentar as pesquisas de gerenciamento de organização. O conceito mais básico e adotado é o de que a cultura organizacional é o modo como as coisas são feitas na organização (DEAL E KENNEDY, 1982).

Ao se introduzir o fator tempo à definição de cultura, tem-se que "cultura é o método habitual de fazer as coisas ao longo do tempo" (CHEN, MEDLIN *et al.*, 2008, p. 361). Assim, é possível dizer que a cultura é o produto da aprendizagem e não da herança (HOFSTEDE, 1993), e "o homem é o resultado do meio cultural em que foi socializado, ele é o herdeiro de um grande processo acumulativo que reflete o conhecimento e a experiência adquiridas pelas numerosas gerações que o antecederam" (LARAIA, 2001, p. 45).

Quando aplicado o conceito de cultura à organização, verifica-se que o grupo social da organização forma a sua cultura

própria. Portanto, cada organização desenvolve sua cultura a partir de seu próprio conjunto de características e valores (CHEN, MEDLIN *et al.*, 2008). Esses valores "representam uma manifestação de cultura que significa crenças adotadas identificando o que é importante para um grupo cultural particular", que, no caso deste estudo, é a organização (LEIDNER E KAYWORTH, 2006, p.356).

A organização vai, então, estruturar regras de atitudes e comportamentos por meio de políticas que retratem os propósitos da empresa e que busquem garantir a sua eficiência. Essa estruturação torna-se mais complexa quanto maior for a organização, haja vista o número elevado de funcionários e a dificuldade em se manter um boa e direta comunicação entre os funcionários e a alta administração (VON SOLMS e VON SOLMS, 2004).

Em busca de uma definição de cultura organizacional, Cadle e Yeates (2008, p. 29) também contribuem com a inclusão da aceitação tácita coletiva. Para os autores a cultura organizacional "reflete as suposições subjacentes sobre como o trabalho é feito, o que é aceitável e o que não é; comportamentos e ações que são encorajados e desencorajados". Ressalta-se, ainda, que essas regras comportamentais são, em sua maioria, não escritas e que se trata de uma força onipresente que controla os comportamentos e atitudes nas organizações (CONNOLLY e LANG, 2013).

Das definições de cultura propostas pelos pesquisadores, entende-se que Schein (2004, p. 17) apresenta a definição que melhor se aplica no campo deste estudo:

Um padrão de pressupostos básicos compartilhados que foi aprendido por um grupo uma vez que resolveu os problemas de adaptação externa e integração interna, que tem funcionado bem o suficiente para ser considerado válido e, portanto, a ser ensinado a novos membros como a forma correta de perceber, pensar e sentir em relação a esses problemas. (tradução do autor)

Em sua definição, o autor demonstra que uma das características da cultura organizacional é a preocupação com a sobrevivência e a continuidade da empresa e vai ao encontro dos demais pesquisadores quando concorda que o desenvolvimento de uma

cultura organizacional é o resultado de um processo complexo de aprendizagem em grupo (SCHEIN, 2004).

No mesmo sentido, Deal e Kennedy (1982) acreditam que a cultura é o fator de maior importância e é responsável pelo sucesso ou o fracasso de uma organização. Trata-se de um fator crítico uma vez que é uma força motriz que impulsiona a organização, que afeta o comportamento dos seus funcionários e o sucesso de suas iniciativas e políticas (VROOM e VON SOLMS, 2004; THOMSON e VON SOLMS, 2006; CHANG e LIN, 2007).

Assim, pode-se dizer que a cultura está para a organização como a personalidade está para um indivíduo. Dela fazem parte os objetivos, as crenças, os pressupostos, os valores e até a forma como as pessoas se vestem e agem. Assim, a coexistência da cultura e da organização leva os pesquisadores a questionarem se a cultura é algo que a organização “tem” ou “é” (CORRISS, 2010).

Adotando uma linguagem própria de tecnologia da informação, pode-se dizer que a cultura organizacional tem um papel de "sistema operacional" da organização. É a sua alma, a sua essência. Representa a mídia, o suporte no processo de comunicação entre gerenciamento e comportamento organizacional dos seus membros (HAGBERG e HEIFETZ, 1997; CHENG, LI *et al.*, 2007).

Por fim, pode-se concluir que a cultura da organização é o saber coletivo tácito, fundamentado nos pressupostos básicos que determinam o comportamento aceitável do grupo, a aquisição e a disseminação dos hábitos e conhecimentos, a fim de garantir a sobrevivência e a eficiência da organização.

2.3.1 Estrutura da Cultura Organizacional

Durante o desenvolvimento das pesquisas sobre a cultura organizacional, verificou-se que alguns autores propuseram estruturá-la ou organizá-la em modelos que explicassem a sua composição ou a sua topologia. A estrutura mais referenciada é a de Schein (2004). O autor defende que todas as culturas organizacionais têm três níveis: Artefatos, Crenças e Valores Compartilhados, e Pressupostos Básicos.

O primeiro nível - Artefatos - representa o nível mais externo. Nele está tudo que pode ser observado, visto e sentido,

como os objetos, arquitetura, manifestações artísticas, tecnologias e produtos, etc. Esse nível tem como principal característica a fácil observação, embora seu significado seja de difícil entendimento ou interpretação.

No segundo nível - Crenças e Valores Compartilhados - são estabelecidos os valores, os elementos oficiais da organização. São exemplos de valores a missão, o objetivo, o planejamento estratégico, os princípios, as políticas, a ética e a visão da organização.

O terceiro nível - Pressupostos Básicos - como o próprio nome sugere, representa o reconhecimento de uma conduta bem sucedida. Ocorre quando os membros do grupo passam a aceitar a conduta como sendo uma verdade e essa passa a compor um pressuposto básico. Tais pressupostos são tácitos e existem a nível individual (ALNATHEER e NELSON, 2009).

A figura 1 abaixo representa os 3 (três) níveis da estrutura da cultura organizacional, propostos por Schein (2004):

Figura 1 - Níveis da Estrutura da Cultura Organizacional



Fonte: (SCHEIN, 2004, p. 21, Edição do autor)

Outros pesquisadores categorizaram a cultura organizacional em função de seus valores, dimensões ou de seus traços culturais. Optou-se por citá-los, resumidamente, por comporem a revisão bibliográfica, em que pese não terem sido escolhidos para aplicação no presente estudo:

- Quinn e Spreitzer (1991), classifica a cultura organizacional em quatro tipos: cultura grupal, cultura de desenvolvimento, cultura hierárquica e cultura racional.

- Brady (2004) classificou em quatro tipos (cultura de clãs, cultura de hierarquia, cultura de adesão e cultura de mercado);

- Denison, Haaland *et al.* (2004) identificaram quatro traços culturais encontrados na cultura organizacional (missão, consistência, adaptabilidade e envolvimento); e

- Kraemer e Carayon (2005) falam em seis dimensões da cultura organizacional.

Em seguida, dando continuidade a parte conceitual do estudo, são abordadas as definições de segurança da informação e, por fim, de cultura organizacional de segurança da informação e, em conclusão, este autor propõe a sua própria definição.

2.4 SEGURANÇA DA INFORMAÇÃO

É sabido que a globalização conectou a humanidade e a tecnologia da informação passou a fazer parte no cotidiano da vida moderna permitindo o aparecimento da sociedade da informação, onde a informação permeia todos os aspectos das vidas, sejam elas profissionais, comerciais ou privadas (VAN NIEKERK E VON SOLMS, 2010).

A necessidade crescente de dados e informações na sociedade da informação vem fazendo com que as organizações acelerem o ritmo de implantação e desenvolvimento tecnológico em busca de um diferencial competitivo. Este cenário fez com que as organizações passassem a adotar iniciativas para regulamentar, padronizar e impor níveis elevados de segurança da informação (PARSONS, YOUNG *et al.*, 2015).

A informação é, portanto, um bem fundamental para a continuidade dos negócios das organizações. Ela carrega consigo um valor agregado e integra seu patrimônio intangível, configurando-se em verdadeiros ativos, ou seja, a sua proteção é extremamente importante (THOMSON e VON SOLMS, 2005; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a).

Entende-se importante, neste ponto, diferenciar Segurança de Segurança da Informação. A segurança é o processo que visa a redução de riscos ou ameaças que podem afetar uma organização. Já a segurança da informação é um requisito de negócios. Seu

objetivo é proteger o investimento da organização nas informações, ou seja, em seus ativos, em seu patrimônio (RASHID, ZAKARIA *et al.*, 2013).

Tem-se, logo, que a segurança da informação é uma área complexa do conhecimento que envolve várias subáreas, cada uma com um perfil específico, o que possibilita uma diversidade de definições disponíveis sobre o tema. O *Committee on National Security Systems* (CNSS) define segurança da informação como “a proteção de informações e sistemas de informação de acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de proporcionar confidencialidade, integridade e disponibilidade.” (COMMITTEE ON NATIONAL SECURITY SYSTEMS, 2015, p. 64).

Anderson (2003) acredita que um dos grandes problemas da segurança da informação decorre da falta de definição ou da forma como a segurança da informação é definida. Ele propôs uma definição na qual, segundo ele, a segurança da informação não é uma simples aplicação dos princípios que fundamentam a segurança da informação, mas procura levar em consideração o equilíbrio entre riscos e controle. Disse ele tratar-se de “um senso bem informado de garantia de que os riscos e controles da informação estão em equilíbrio” (ANDERSON, 2003, p. 310, tradução do autor).

Para mitigar os riscos e aumentar os controles é indispensável uma governança de segurança da informação na organização (DA VEIGA e ELOFF, 2007). O envolvimento da alta gerência definindo e propondo políticas, procedimentos e responsabilidades de segurança incentiva os colaboradores a adotarem comportamentos éticos adequados e a cumprirem os padrões organizacionais (MARTINS e ELOFF, 2002; DOJKOVSKI, LICHTENSTEIN *et al.*, 2010).

Para este estudo, optou-se por adotar as definições constantes nos normativos que disciplinam a matéria no âmbito da legislação brasileira, a seguir descritas.

A Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, define a Segurança da Informação e Comunicações como “ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações” (BRASIL, 2008).

As normas NBR ISO/IEC 17799:2005 e 27001:2005 definem segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. ix).

O Decreto 3.505, de 13 de junho de 2000, é mais abrangente ao definir a Segurança da Informação como:

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 ao seu desenvolvimento.

Basicamente as definições de segurança da informação apresentam um núcleo comum que é a continuidade dos negócios e a soberania da organização. Também se pode observar que praticamente todas as definições baseiam-se nos princípios/propriedades da segurança da informação descritos na NBR ISO/IEC 27001:2013 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a) São três os princípios que fundamentam o conceito da SI:

O princípio da Confidencialidade que garante ao usuário que “a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a, p. 2).

A Integridade é a propriedade de salvaguarda da exatidão e completeza de ativos. Ele garante ao usuário a fiel representação da informação, garantindo que o conteúdo não foi modificado, violado ou alterado indevidamente (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a, p. 3).

A Disponibilidade representa "a propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada." Garante ao usuário que a informação estará disponível no mo-

mento em que for necessário (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a, p. 2).

Embora algumas literaturas dos organismos normatizadores acrescentem mais quatro princípios: Autenticidade, Responsabilidade, Não-Repúdio e Confiabilidade (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a; RASHID, ZAKARIA *et al.*, 2013), o estudo se suporta nos três princípios referidos anteriormente.

Os três grandes princípios que fundamentam a S.I. abrangem, por sua vez, três subdomínios: tecnologia, processos e pessoas. A tecnologia é o subdomínio responsável pela implementação de recursos que envolvem basicamente o desenvolvimento de Hardwaree Software, como por exemplo, Senhas, Biometria, *Firewall* e Antivírus. Essas técnicas não asseguram por si só a informação, pois sua aplicação depende do profissional envolvido. Os processos são caracterizados e fundamentados pelos procedimentos aplicados à proteção da informação, tais como elaboração de políticas de segurança, normatizações das operações, relatórios de incidentes, registro e revogação de usuários. Mas elaborar, simplesmente, um conjunto de medidas e procedimentos não assegura a informação, pois para a sua correta operação se necessitam de pessoas comprometidas com a organização. As pessoas, por sua vez, devem ser consideradas em todos os processos, haja vista que o problema de segurança não é simplesmente um problema técnico-normativo.

Praticamente todos os processos decorrentes dos princípios da SI e dos subdomínios necessários para proteger a organização de incidentes são, em grande parte, dependentes do comportamento humano. Os colaboradores da organização são a maior ameaça à segurança da informação, seja de forma intencional ou por omissão ou negligência (MITNICK e SIMON, 2002; VAN NIEKERK e VON SOLMS, 2010).

Uma vez compreendido que a segurança da informação é um conjunto de princípios, tecnologias, processos e pessoas, é claro que, em um nível de abstração mais elevado, trata-se de um problema de gerenciamento da organização (LIM, AHMAD *et al.*, 2010).

A segurança da informação é, sobretudo, um problema de pessoas (PARSONS, MCCORMAC *et al.*, 2014). Assim, os as-

pectos humanos e sociais envolvidos nos processos organizacionais, como responsabilidade, conhecimento, orientação, liderança, ética e democracia, devem ser considerados quando se tratar da segurança da informação (DA VEIGA, MARTINS *et al.*, 2007; VAN NIEKERK e VON SOLMS, 2010; ASTAKHOVA, 2014).

2.4.1 Segurança da Informação e Segurança Cibernética

Não se pode falar de segurança da informação sem falar em segurança cibernética e a diferenciação entre elas. Enquanto que a SI, conforme visto anteriormente, objetiva a manutenção da confidencialidade, integridade e disponibilidade de dados e/ou serviços no ambiente da organização, a segurança cibernética tem abrangência maior, pois define segurança da informação em um contexto de espaço cibernético - ciberespaço.

O Ciberespaço é “um ambiente complexo resultante da interação de pessoas, software e serviços na Internet, apoiado por dispositivos de tecnologia física e de comunicações distribuídas em todo o mundo (TIC) e redes conectadas” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2015, p. 5).

A segurança cibernética está, portanto, em uma camada superior de abstração. Ela engloba a segurança da informação, a segurança das pessoas enquanto seres humanos e a segurança do Estado. No nível do elemento humano a segurança cibernética considera o homem como um alvo potencial de ataques. Cita-se o *cyberbullying*, um ataque à integridade humana, ou o Ciberterrorismo, que é um ataque em grande escala ou em nível de nação. Ele atenta contra a infraestrutura, rede elétrica, usinas nucleares, abastecimento, etc. A segurança cibernética está voltada para mecanismos de proteção com vistas à manutenção da soberania do Estado (ONU, 2004; 2010; VON SOLMS e VAN NIEKERK, 2013).

2.4.2 Fator Humano

Ao longo do estudo, vem se consolidando a importância do homem e sua influência no gerenciamento da segurança da informação. Embora a literatura aborde com mais ênfase as questões técnicas que ameaçam a SI, há um reconhecimento crescente do fator humano como uma importante fonte também de ameaça

(VROOM e VON SOLMS, 2004; FURNELL, JUSOH *et al.*, 2006; PARSONS, YOUNG *et al.*, 2015)

Como visto, o homem é o elo mais fraco da cadeia da segurança da informação, não somente por carregar consigo uma cultura "prévia" que pode não se alinhar aos valores da organização, mas, também, pelo fato de estar muitas vezes alheio à política e à estratégia da empresa a qual pertence. Estudos revelam que esse envolvimento de todos os colaboradores, nos diversos níveis, é crucial para o sucesso na segurança da rede de informações (VROOM e VON SOLMS, 2004; PARSONS, YOUNG *et al.*, 2015)

As redes de informações das organizações estão vulneráveis, de forma direta e constante, ao fator humano, às decisões e ações de seus colaboradores. Quer seja de forma deliberadamente maliciosa, quer seja de forma ingênua. Os "erros" humanos, ensinada a literatura, são a maior causa de violação da segurança da informação (PARSONS, YOUNG *et al.*, 2015).

Nessa linha, outros autores afirmam que a "segurança comportamental" é o segredo para um gerenciamento bem sucedido da segurança do sistema de informação da organização, pois a maioria das violações de segurança tecnológica ocorre porque os funcionários internos de uma organização corrompem, de alguma forma, os controles existentes (DHILLON, 2001).

Não se pode desprezar que a maioria desses controles tem problemas operacionais que dependem do comportamento humano (THOMSON e VON SOLMS, 2006) e, portanto, não são suficientes para garantir a segurança das informações. Como bem disseram Mitnick e Simon (2002, p. 79) "Não confie em garantias de rede e *firewalls* para proteger suas informações. Olhe para o seu ponto mais vulnerável. Você encontrará geralmente que a vulnerabilidade está em suas pessoas".

Daí reforça-se a importância da participação da alta administração nas atividades relacionadas a SI, na formação de uma cultura organizacional baseada em regras bem definidas e conhecidas para garantir que os funcionários adquiram comportamentos que reduzam os riscos de atitudes negligentes ou maliciosas (THOMSON e VON SOLMS, 2005; HU, DINEV *et al.*, 2008; PONEMON INSTITUTE, 2012).

Conclui-se, assim, que qualquer tentativa de uma organização de implementar controles de segurança da informação baseados apenas em tecnologias se mostra prejudicada ou fadada ao fracasso se não se considerar o fator cultural da organização (THOMSON e VON SOLMS, 2006).

Procurando mitigar o efeito humano e influenciar positivamente o comportamento e a atitude dos funcionários, as organizações têm investido na adoção de políticas e procedimentos de segurança da informação e, principalmente, na educação, treinamento e informação. Essa atitude das organizações está apoiada na Teoria do Comportamento Planejado – TCP (ou TPB, se no idioma inglês), e no modelo de Conhecimento Atitude Comportamento – CAC (ou KAB, se no idioma inglês), onde partem do pressuposto que o acúmulo do conhecimento muda as atitudes e, que essas mudanças nas atitudes promovem a mudança de comportamento. O conhecimento também influencia em um melhor desempenho e uma melhor conformidade comportamental com as políticas de segurança da informação (AJZEN, 1991; MILLER, 2010; PARSONS, YOUNG *et al.*, 2015).

Eis aí o maior desafio do estudo, considerar o fator humano na avaliação da cultura como principal ator no gerenciamento da segurança da informação.

2.5 CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

A leitura dos tópicos anteriores permitiu a compreensão do que vem a ser cultura, cultura da organização e segurança da informação. Cabe, portanto, convergir esses conceitos de modo a obter uma adequada definição de cultura organizacional de segurança da informação, objeto que o estudo se propõe a avaliar.

No entanto, antes mesmo de se pensar em cultura organizacional de segurança da informação deve-se expor os conceitos de cultura de segurança e cultura de segurança da informação.

Ao pesquisar as definições de cultura de segurança na literatura, chega-se a uma definição abrangente na qual cultura de segurança é uma consequência do compartilhamento de valores, atitudes, percepções, crenças, competências e padrões individuais e de grupo (JOHNSEN, HANSEN *et al.*, 2006; MALCOLMSON, 2009).

Para se estabelecer uma cultura de segurança é necessária uma mudança da atual cultura do indivíduo ou do grupo. Isso significa dizer que a pessoa tem que alterar comportamentos e atitudes de modo a demonstrar uma conscientização voltada à segurança (NGO, ZHOU *et al.*, 2005).

É nítida a rápida evolução e o crescimento da utilização dos sistemas e redes de informação na atual sociedade. Agregado a isso, tem-se uma população interconectada, com acesso em tempo real a uma ampla rede de informações. Essa interconectividade se verifica presente tanto nas relações profissionais, quanto nas pessoas, exigindo, assim, uma preocupação gradual na segurança, confiabilidade, rapidez e atualizações desses sistemas de informações que se mostram cada dia mais expostos e, logo, vulneráveis a ameaças internas e externas aos sistemas que podem causar danos à segurança.

A vulnerabilidade a que estão sujeitos os sistemas de informação requer, conforme já dito, uma urgente conscientização dos desenvolvedores, fornecedores, gerentes, usuários, enfim, dos participantes desses sistemas quanto à necessidade de desenvolvimento de uma cultura de segurança da informação, com o objetivo de identificar os riscos e minimizar os danos (OCDE, 2002).

Segundo Johnson e Goetz (2007) a segurança geral de uma organização é o resultado das ações de cada indivíduo. Sendo assim, o estabelecimento da consciência de segurança pelos membros da organização é fundamental para o sucesso do processo de aculturação em segurança da informação na organização.

É, portanto, a cultura de segurança que propiciará a implementação de políticas e práticas de segurança da informação nas organizações e, conseqüentemente, deve ser esse o objetivo da organização: criar uma cultura efetiva de segurança da informação no âmbito de seu estabelecimento (ALNATHEER e NELSON, 2009). Uma cultura de segurança representa um dos fundamentos necessários para o gerenciamento da segurança da informação na organização. Essa cultura só pode ser alcançada por meio da capacitação e da conscientização dos colaboradores (FURNELL, 2007).

Considerando que as organizações são formadas por pessoas e totalmente dependentes delas, é imprescindível direcionar

os estudos e a revisão bibliográfica para a definição e o estabelecimento de diretrizes que fortaleçam a cultura de segurança da informação na organização, bem como de princípios que permitam a sua avaliação.

O tema da cultura de segurança da informação é uma preocupação constante da Organização para a Cooperação e Desenvolvimento Econômico - OCDE. Em 2002, essa organização reeditou o documento *Guidelines for the Security of Information Systems*, de 1992, sob novo título: "Diretrizes para a Segurança de Sistemas e Redes de Informação. Rumo a uma Cultura de Segurança" (OCDE, 2002, tradução do autor). Esse documento estabelece as diretrizes que devem ser observadas para se promover uma cultura de segurança da informação nas organizações. Essas diretrizes "propõem a todos os participantes que adotem e promovam uma 'cultura de segurança' como forma de pensar, avaliar e agir na operacionalização dos sistemas e redes de informação" (OCDE, 2002, p. 8, tradução do autor).

Para tanto, as diretrizes se baseiam em nove princípios que levam em consideração o fato de se tratar de um contexto que está em permanente mudança, a dependência das pessoas nos sistemas de informação, os meios de comunicação e serviços os quais precisam ser confiáveis e seguros e na importância de envolver todos os participantes na formação e na promoção de uma cultura de segurança. A OCDE enfatiza que as melhores práticas para a implantação da cultura de segurança da informação são aquelas em que todos os participantes (colaboradores) compreendem os requisitos de segurança e as questões (soluções, decisões) são temas de interesse e responsabilidade em todos os níveis da organização (OCDE, 2002).

Inicialmente, destacam-se os objetivos das diretrizes definidas pela OCDE (2002, p. 8/9, tradução do autor) para o desenvolvimento de uma cultura de segurança nas organizações:

- Promover uma cultura de segurança, entre todos os participantes, como um meio de proteger os sistemas e redes de informação.

- Aumentar a conscientização sobre os riscos para os sistemas e redes de informação, sobre as políticas, práticas, medidas e procedimentos disponíveis para enfrentar esses riscos, bem como a necessidade de adotá-las e implementá-las.

- Promover, para os participantes, uma maior confiança nos sistemas e redes de informação e na forma como eles são disponibilizados e utilizados.

- Criar um quadro geral de referência que ajude os participantes a compreender a natureza dos problemas relacionados à segurança e a respeitar os valores éticos na elaboração e implementação de políticas, práticas, medidas e procedimentos coerentes para a segurança dos sistemas e redes de informação.

- Promover, entre os participantes, a cooperação e o compartilhamento de informações adequadas para a formulação e implementação de políticas, práticas, medidas e procedimentos de segurança.

- Promover a conscientização da segurança enquanto objetivo importante para todos os participantes envolvidos na elaboração e implementação das normas.

Em seguida, a OCDE estabelece nove princípios que devem ser observados para se implementar uma cultura de segurança da informação nas organizações: Sensibilização (Consciência), Responsabilidade, Resposta (Reação), Ética, Democracia, Avaliação de risco, Projeto de Segurança e Implementação, Gestão de Segurança e Reavaliação (OCDE, 2002, p. 9/12).

Não existe uma ordem ou hierarquia entre os princípios. Eles devem ser considerados como um todo, pois suas diretrizes sevem para todos os níveis, incluindo desde o político até o operacional. Assim, cada membro da organização está sob as mesmas diretrizes com níveis de responsabilidade compatíveis com sua posição, e todos são auxiliados pelos fatores consciência, educação, compartilhamento de informações e natureza da formação, a fim de facilitar uma melhor compreensão das questões relacionadas à segurança e a adoção de melhores práticas (OCDE, 2002).

Os nove princípios estabelecidos pela OCDE constituem o suporte referencial para a elaboração do instrumento de avaliação da cultura organizacional de segurança da informação deste trabalho. Assim, o próximo tópico deste capítulo se dedica a detalhar os princípios, definindo-os e citando, para cada um deles, a fundamentação teórica revisada na literatura.

2.6 PRINCÍPIOS DIRETIVOS DE UMA CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

Os princípios estabelecidos pela OCDE no documento "Diretrizes para a Segurança de Sistemas e Redes de Informação. Rumo a uma Cultura de Segurança" (OCDE, 2002, tradução do autor) estão listados a seguir, detalhados conforme o documento original e traduzidos pelo autor. Em cada descrição do princípio, são abordadas, também, algumas considerações e/ou definições de autores que pesquisaram o tema relacionado.

2.6.1 Sensibilização (Consciência)

Os participantes devem estar cientes da necessidade de garantir a segurança dos sistemas e redes de informação e do que podem fazer para melhorar a segurança (OCDE, 2002, p. 8, tradução do autor, grifo no original).

A consciência dos riscos e das soluções disponíveis é a primeira linha de defesa para garantir a segurança dos sistemas e redes de informação. Os sistemas e redes de informação podem estar expostos a ambos os riscos internos e externos. Os participantes devem entender que as falhas de segurança podem afetar significativamente os sistemas e redes sob seu controle, bem como os dos outros, devido à interconectividade e interdependência dos sistemas. Os participantes devem estar cientes da configuração e das atualizações disponíveis para o seu sistema, o lugar que ocupa nas redes, de boas práticas que podem implementar para melhorar a segurança, bem como das necessidades dos outros participantes (OCDE, 2002, p. 8, tradução do autor).

Com respeito a este princípio, destaca-se a necessidade de conscientização dos colaboradores quanto à segurança. Siponen (2000) descreve que os usuários dos sistemas de informação devem estar conscientes da missão de segurança. Ele identifica duas categorias de consciência de segurança, uma de estrutura, assim chamada aquela que envolve os aspectos de padronização, certifi-

cação, regras, medições, e a outra de conteúdo, que engloba a orientação, motivação, incentivo e consciência propriamente dita. A cultura de segurança na organização só pode ser alcançada por meio da capacitação e da conscientização dos colaboradores (FURNELL, 2007).

Em Lim, Ahmad *et al.* (2010), os autores reforçam a ligação e a dependência entre a cultura de segurança da informação e as ações da alta administração, como a delineação objetiva de responsabilidades, destinação de recursos para investimento em programas de conscientização e em práticas de segurança. O conhecimento da cultura organizacional é muito importante no processo de desenvolvimento, conhecimento e crença na cultura de segurança da informação.

Ao embutir nas pessoas uma consciência de segurança, acredita-se que há uma mudança comportamental que fomenta o estabelecimento de uma cultura de segurança da informação (NGO, ZHOU *et al.*, 2005).

2.6.2 Responsabilidade

Todos os participantes são responsáveis pela segurança dos sistemas e redes de informação (OCDE, 2002, p. 10, tradução do autor, grifo no original).

Os participantes dependem de sistemas e redes de informação locais e mundiais interconectados e devem compreender a sua responsabilidade pela segurança desses sistemas e redes. Eles devem prestar contas na razão de suas funções individuais. Os participantes devem, regularmente, rever e avaliar suas próprias políticas, práticas, medidas e procedimentos para se assegurarem que estão adequados ao seu ambiente. Aqueles que desenvolvem, projetam e fornecem produtos e serviços devem considerar a segurança dos sistemas e redes e divulgar as informações adequadas, incluindo atualizações em tempo hábil, para que os usuários sejam capazes de entender a funcionalidade de segurança dos produtos e serviços e suas responsabi-

lidades relacionadas à segurança (OCDE, 2002, p. 10, tradução do autor).

Paralelamente ao rápido desenvolvimento e aperfeiçoamento de tecnologias da informação, verifica-se o crescimento da prática de atos reprováveis, como o uso indevido de dados, incluindo a cópia não autorizada, a extorsão e o roubo. Essas práticas demonstram uma falta de responsabilidade comportamental e profissional do infrator e a solução efetiva desse problema depende do nível da cultura de segurança da informação dos participantes nas relações de informação.

Os sujeitos pertencentes às relações de informação devem ter responsabilidade e ética comportamental no ambiente de informação, pois "novas tecnologias de informação criam não só novas oportunidades comuns, mas também vulnerabilidades comuns, que constituem uma responsabilidade comum" (ASTAKHOVA, 2014, p. 27).

Nesse sentido, Rashid, Zakaria *et al.* (2013) colocam que a consciência da proteção e da segurança da informação é responsabilidade de todos os usuários da informação. Essa responsabilidade deve estar explícita e compreendida por todos os participantes, no âmbito de suas atribuições (CHIA, MAYNARD *et al.*, 2002; DOJKOVSKI, LICHTENSTEIN *et al.*, 2010). Nas organizações, cabe a alta administração assumir a responsabilidade pela definição, comunicação, treinamento e educação da cultura de segurança da informação com vistas a alcançar o nível de cultura desejado (VON SOLMS e VON SOLMS, 2004; THOMSON e VON SOLMS, 2005; DA VEIGA e ELOFF, 2007; MCCOY, STEPHENS *et al.*, 2009).

2.6.3 Resposta (Reação)

Os participantes devem agir em tempo hábil e de maneira cooperativa para prevenir, detectar e responder a incidentes de segurança (OCDE, 2002, p. 10, tradução do autor, grifo no original).

Reconhecendo a interconectividade dos sistemas e redes de informação e o potencial de danos que se alastram rapidamente e de forma generalizada, os participantes devem reagir prontamente e com um espírito de cooperação aos incidentes de segu-

rança. Eles devem compartilhar as informações sobre ameaças e vulnerabilidades, conforme apropriado, e implementar procedimentos para uma cooperação rápida e efetiva a fim de prevenir, detectar e responder a incidentes de segurança. Onde for permitido, isso pode implicar em compartilhamento de informações e cooperação além das fronteiras (OCDE, 2002, p. 10, tradução do autor).

A cultura de segurança da informação surge do incentivo na adoção de um comportamento aceitável de segurança da informação. Logo, em toda organização a cultura de segurança da informação representa a forma como as pessoas reagem em relação a informação e a sua segurança. Os procedimentos que os participantes envolvidos nos sistemas de informação costumam adotar em seu trabalho diário podem indicar as vulnerabilidades do sistema e mostrar quais respostas a essas vulnerabilidades devem ser implementadas de modo a reforçar a cadeia de segurança da informação (MARTINS e ELOFF, 2002).

As ações tomadas pela organização para a proteção da informação vão orientar o desenvolvimento de uma cultura organizacional de segurança da informação (DA VEIGA e ELOFF, 2007).

2.6.4 Ética

Os participantes devem respeitar os interesses legítimos de outros participantes (OCDE, 2002, p. 11, tradução do autor, grifo no original).

Dada a onnipresença dos sistemas e redes de informação em nossas sociedades, os participantes precisam reconhecer o quanto sua ação ou omissão pode prejudicar os outros. A conduta ética é, portanto, crucial e os participantes devem se esforçar para desenvolver e adotar as melhores práticas e promover comportamentos que reconheçam a necessidade de segurança e respeitem os interesses legítimos dos outros participantes (OCDE, 2002, p. 11, tradução do autor).

As boas práticas existentes em uma organização representam a cultura estabelecida na corporação. É necessário, portanto, a prática de um comportamento ético, de uma conduta cotidiana ética em relação à segurança da informação (MARTINS E ELOFF, 2002). Essa conduta ética não pode ser somente a ética formalizada, escrita, mas sim aquela compartilhada e vivenciada pela cultura organizacional (LOWRY, POSEY et al., 2014).

Segundo Trompeter e Eloff (2001, p. 386) o conceito de ética ou consciência sócio ética, no contexto organizacional, pode ser definido como "a conformidade de uma organização com os princípios éticos de segurança da informação reconhecidos". A utilização da ética no ambiente da informação tem por finalidade a identificação dos aspectos que envolvem os conceitos de bem e mal, para, assim, definir os padrões éticos aceitáveis de segurança da informação (RUIGHAVER, MAYNARD et al., 2010).

2.6.5 Democracia

A segurança dos sistemas e redes de informação deve ser compatível com os valores essenciais de uma sociedade democrática (OCDE, 2002, p. 11, tradução do autor, grifo no original).

A segurança deve ser implementada de forma consistente com os valores reconhecidos pelas sociedades democráticas, notadamente a liberdade de troca de pensamentos e ideias, o livre fluxo de informações, a confidencialidade da informação e da comunicação, a proteção adequada dos dados pessoais, a abertura e a transparência (OCDE, 2002, p. 11, tradução do autor).

Os autores Hu, Dinev et al. (2012, p. 10) defendem a participação da alta administração nas iniciativas de segurança da informação para incentivar uma cultura organizacional de segurança da informação. Esse envolvimento da alta gerência, definida como liderança e necessária para o estabelecimento da democracia, vai incentivar um comportamental adequado e participativo dos colaboradores e, conseqüentemente, vai favorecer o cumprimento das políticas de segurança da informação, influenciando diretamente na cultura organizacional.

Percebe-se uma forte relação entre cultura organizacional e liderança organizacional na medida em que a própria cultura

organizacional é definida pela alta administração e pode ser por ela manipulada (SCHEIN, 2004). Esse argumento reforça a necessidade da cultura organizacional refletir valores que os participantes compartilhem para que haja uma livre aderência (MALCOLMSON, 2009). Uma mudança de cultura só será aceita se a coletividade entender que se trata de uma nova boa prática que dará certo.

Em Lowry, Posey *et al.* (2014), os estudos demonstraram que quanto mais coletivo for o grupo menor a chance de ocorrerem incidentes de segurança, enquanto que em grupos onde as pessoas são mais individualistas há uma tendência a aumentar os incidentes. Entende-se, portanto, que o ambiente democrático é propulsor da implementação da cultura organizacional de segurança da informação. As políticas de segurança para serem aceitas e cumpridas pelos membros do grupo não podem infringir ou agredir os valores e crenças individuais (VON SOLMS e VON SOLMS, 2004).

2.6.6 Avaliação de risco

Os participantes devem realizar avaliações de risco (OCDE, 2002, p. 11, tradução do autor, grifo no original).

A avaliação de riscos possibilita identificar ameaças e vulnerabilidades e deve ser suficientemente ampla para abranger o conjunto dos principais fatores internos e externos, tais como tecnologia, fatores físicos e humanos, políticas e serviços de terceiros que influenciam na segurança. A avaliação de riscos permitirá determinar o nível de risco aceitável e auxiliar na seleção de medidas de controles adequados para gerenciar o risco de danos potenciais aos sistemas e redes de informação, tendo em conta a natureza e importância da informação a ser protegida. Devido à crescente interconectividade dos sistemas de informação, a avaliação de riscos deve considerar os danos potenciais que podem ser originados por terceiros ou causados a terceiros (OCDE, 2002, p. 11, tradução do autor).

Para Martins e Eloff (2002), todos os colaboradores da organização precisam perceber o risco e assumir, como uma atividade cotidiana do trabalho, a análise do risco. A incorporação dessa atividade integra a cultura de segurança da informação.

Para conceituar risco, sugere-se a definição trazida pela norma NBR ISO/IEC 27005: "o efeito da incerteza nos objetos" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011, p 3).

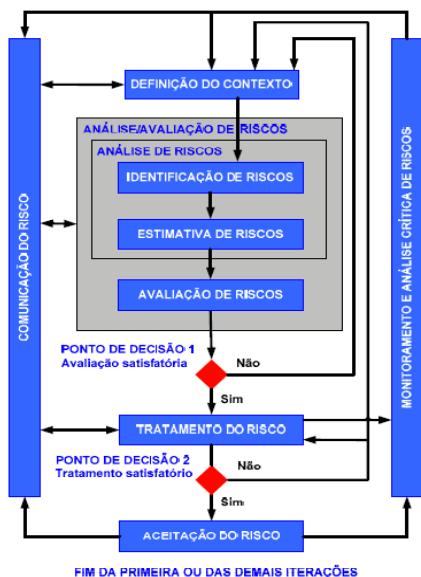
No livro de Pressman, ao dispor da identificação dos riscos no planejamento de projetos (PRESSMAN, 1995, p. 131), o autor cita a valiosa afirmativa de Peter Drucker: "Embora seja fútil tentar eliminar o risco e questionável tentar minimizá-lo, é fundamental que os riscos assumidos sejam os riscos certos". E nada mais apropriado para a identificação e avaliação dos riscos certos do que a adoção da gestão de risco.

A Gestão de Risco ou Gerenciamento do Risco pode ser considerado como o processo de administrar exclusivamente o risco (DIAS, CALIL *et al.*, 2011). Na norma NBR ISO/IEC 27005 tem-se que a gestão do risco é o conjunto de "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011, p. 5).

O processo de administrar o risco visa desenvolver procedimentos de análise, tratamento, aceitação e comunicação do risco. Trata-se de uma metodologia constituída por um conjunto de procedimentos e técnicas organizadas, com o objetivo de gerir sistemas técnicos, humanos e ambientes (DIAS, CALIL *et al.*, 2011).

Cabe, aqui, transcrever o diagrama apresentado pela norma NBR ISO/IEC 27005 onde estão sintetizados os passos e componentes envolvidos no processo de gestão do risco de segurança da informação. Trata-se de uma evolução do diagrama especificado na NBR ISO 31000:2009, que propõe um modelo interativo na execução do processo de avaliação dos riscos.

Figura 2 - Processo de gestão de riscos de segurança da informação



Fonte: (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011, p. 9)

O processo de gestão de risco acima proposto permite minimizar o tempo e o esforço despendidos na identificação de controles. Ele inicia-se com a definição do contexto, que poderá ser interno ou externo a depender de onde a organização busca atingir seus objetivos. Em seguida, procede-se ao levantamento do risco, identificando-o e estimando-o, para, então, avaliar o risco. Essa etapa produz uma quantidade de informações que devem ser julgadas se são ou não satisfatórias. No caso de não serem satisfatórias, o processo retorna para ser reavaliado. O próximo passo é avaliar se os tratamentos do risco são satisfatórios. Durante o processo de tratamento do risco é gerado o risco residual, ou seja, risco remanescente após seu tratamento. Se o risco residual for aceito então é procedida a comunicação do risco e o seu monitoramento.

A avaliação do risco integra, portanto, a gestão do risco e seu tratamento é fundamental para a adoção de políticas e de mecanismos de proteção da informação que farão parte da cultura de segurança da informação.

2.6.7 Projeto de segurança e implementação

Os participantes devem integrar a segurança como um elemento essencial dos sistemas e redes de informação (OCDE, 2002, p. 12, tradução do autor, grifo no original).

Sistemas, redes e políticas precisam ser devidamente planejados, implementados e coordenados para otimizar a segurança. Um importante foco, mas não exclusivo, desse esforço é a criação e adoção de salvaguardas e soluções para evitar ou limitar danos potenciais de ameaças e vulnerabilidades identificadas. As salvaguardas e soluções devem ser, ao mesmo tempo, técnicas e não-técnicas e devem ser proporcionais ao valor da informação nos sistemas e redes de informação da organização. A segurança deve ser um elemento fundamental do conjunto dos produtos, serviços, sistemas e redes, e deve fazer parte integrante do projeto e da arquitetura dos sistemas. Para os usuários finais, o projeto e a implementação da segurança consistem, essencialmente, na seleção e configuração de produtos e serviços para o seu sistema (OCDE, 2002, p. 12, tradução do autor, grifo no original).

Conforme amplamente relatado, é consenso na literatura a necessidade de envolvimento de todos os participantes (colaboradores) da organização na segurança da informação. Não poderia, portanto, ser diferente quando se trata da concepção (projeto) e da implementação dos sistemas e redes de informação. Não se pode presumir que os participantes detenham o conhecimento suficiente e necessário de segurança da informação relacionada a suas funções do trabalho, de modo a desenvolver suas atividades de forma segura (VAN NIEKERK e VON SOLMS, 2010). Esses colaboradores precisam estar capacitados e conhecerem as boas práticas de segurança, até porque a força de trabalho envolvida em projetos na área de tecnologia da informação costuma se concentrar mais na tecnologia, na ferramenta, do que no planejamento da segurança da informação (JOHNSEN, HANSEN *et al.*, 2006).

Como a informação é um valioso ativo para a organização, e, portanto, precisa ser protegida, é imprescindível que se pense na segurança da informação desde a concepção (projeto) dos sistemas e redes de informação (DA VEIGA e ELOFF, 2007; OKERE, VAN NIEKERK *et al.*, 2012); ()

2.6.8 Gestão de Segurança

Os participantes devem adotar uma abordagem abrangente para a gestão da segurança (OCDE, 2002, p. 12, tradução do autor, grifo no original).

A Gestão ou Gerenciamento da segurança deve basear-se na avaliação dos riscos e deve ser dinâmica e global, de modo a abranger todos os níveis de atividades dos participantes e todos os aspectos de suas operações. Ela deve incluir, também, respostas antecipadas à ameaças emergentes e abordar a prevenção, detecção e respostas a incidentes, a recuperação dos sistemas, a manutenção contínua, o controle e a auditoria. As políticas de segurança dos sistemas e redes de informações, as práticas, medidas e procedimentos em matéria de segurança devem ser coordenados e integrados para criar um sistema de segurança coerente. Os requisitos da gestão de segurança dependem do nível de envolvimento e do papel do participante, dos riscos envolvidos e das características do sistema (OCDE, 2002, p. 12, tradução do autor).

Em uma abordagem mais abrangente, e para efeito de melhor compreensão do que vem a ser a gestão da segurança na visão dos estudiosos no assunto, entende-se oportuno trazer alguns conceitos de governança da segurança e sua relação com a cultura organizacional.

A governança de segurança da informação pode ser definida como um subconjunto do programa de governança da organização (NATIONAL CYBER SECURITY TASK FORCE, 2004). Ao relatar a evolução da cultura organizacional de segurança da informação, tópico 1.1., viu-se que a governança de segurança da informação constitui a quarta e última onda e incorpora, em seu

conceito, a gestão da segurança como um de seus processos (VON SOLMS, 2006).

Thomson e Von Solms (2005) perceberam que, não obstante o valor que a informação tenha para a organização, sua proteção por meio da segurança da informação ainda não representa uma parte significativa dentro da estratégia da governança da organização (governança corporativa). A tendência é que a governança de segurança da informação ocupe seu devido papel na governança corporativa, já que sua principal função é minimizar os riscos de ataques à informação (DA VEIGA e ELOFF, 2007).

Corriss (2010, p. 36, tradução do autor) afirma que "a governança e a gestão da segurança são mais eficazes quando são sistêmicas, entrelaçadas na cultura e tecidas pelos comportamentos e ações organizacionais". Nesse sentido, os estudos de Lim, Ahmad *et al.* (2010) apontam para a importância e o desafio no gerenciamento da cultura de segurança da informação nas organizações, uma vez que os participantes tanto representam ameaças à segurança da informação, quanto são os responsáveis pela proteção desse valioso ativo.

Considerando que a gestão da informação é o instrumento que garante ao gestor a correta e tempestiva tomada de decisão, o *Control Objectives for Information and Related Technologies* - COBIT apresenta um conjunto de ferramentas de boas práticas de governança de tecnologia da informação. O documento, criado pela ISACA - *Information Systems Auditand Control Association*, objetiva o controle da informação, desde o seu planejamento até o monitoramento dos resultados, incluindo indicações do que deve ser feito para se ter uma governança de segurança da informação (VON SOLMS, 2005).

Em 2002 foi publicada a norma ISO/IEC 17799 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. A norma ficou conhecida no Brasil com a abreviação ABNT NBR ISO/IEC 17799. Trata-se de normativo que regulamenta os processos de implantação de um Sistema de Gestão da Segurança da Informação SGSI. Em 2005, a referida norma foi reeditada com algumas melhorias e, posteriormente, renomeada para ISO/IEC 27002. O documento está estruturado, na versão 2013, em 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 contro-

les (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b, p. 1), que serão detalhados no capítulo AVALIAÇÃO DA CULTURA, por constituírem um dos fundamentos teóricos para a elaboração dos itens do instrumento de avaliação.

2.6.9 Reavaliação

Os participantes devem rever e reavaliar a segurança dos sistemas e redes de informação e fazer as modificações apropriadas nas políticas, práticas, medidas e procedimentos de segurança (OCDE, 2002, p. 12, tradução do autor, grifo no original).

Novas vulnerabilidades e ameaças, ou em evolução, são constantemente descobertas. Todos os participantes devem, continuamente, rever, reavaliar e modificar todos os aspectos da segurança para lidar com esses riscos que estão em evolução (OCDE, 2002, p. 12, tradução do autor).

A etapa de reavaliação em um processo representa o momento do ciclo em que se faz uma análise crítica, um monitoramento objetivando implementar melhorias no processo. Para a segurança da informação, essa reavaliação deve ser feita com base em novas ameaças que surgirem e que representem novos fatores de vulnerabilidades que devem ter suas soluções de segurança redimensionadas (ASTAKHOVA, 2014).

A avaliação e reavaliação da cultura de segurança e da governança de segurança são indispensáveis para que a organização fortaleça a sua cultura organizacional (ALNATHEER e NELSON, 2009).

2.7 AVALIAÇÃO DA CULTURA

Não se verificou, na literatura, uma avaliação da cultura de segurança da informação que abordasse, de forma integrada, todos os níveis de cultura de segurança da informação em uma organização, tanto em relação aos colaboradores, quanto em relação aos aspectos subjacentes da cultura e das subculturas (OKERE, VAN NIEKERK *et al.*, 2012). Isto porque a cultura de S.I., conforme amplamente debatido, envolve aspectos subjetivos, tácitos, individuais e coletivos, que requerem uma abordagem multidisciplinar, envolvendo campos do conhecimento como a antropologia, psicologia, tecnologia, administração e gestão, den-

tre outros. Para a avaliação objetiva da cultura tem-se, portanto, que recorrer a um modelo quantitativo capaz de explicar esses aspectos relacionados ao fator humano (PASQUALI, 2009).

Algumas avaliações propostas por pesquisadores apresentam certas limitações que este estudo pretende superar. A abordagem de Schlienger e Teufel (2003), por exemplo, direcionou a avaliação para o pessoal que trabalha com segurança da informação. Essa pesquisa pode não representar qual o real problema de segurança que a organização está enfrentando, pois avalia apenas o subgrupo de colaboradores especializados, não refletindo, portanto, o conhecimento de todos colaboradores da organização.

Já Martins e Eloff (2002) focaram a pesquisa na avaliação das premissas tácitas compartilhadas. Embora o questionário tenha sido direcionado para os colaboradores de todos os níveis da organização, a abordagem não foi capaz de avaliar a cultura de segurança da informação, na sua completude, conforme reconheceram os próprios autores.

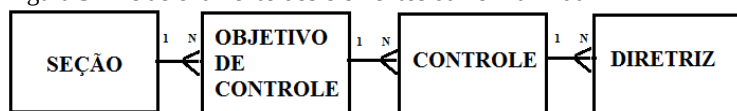
A avaliação, portanto, não pode estar sujeita à interpretação pelos respondentes e deve permitir sua aplicação em qualquer tipo de organização, de modo a garantir a confiabilidade e a validade do instrumento de medida da cultura e a comparabilidade entre organizações (SCHEIN, 2009). Assim, este estudo busca estruturar a avaliação da cultura organizacional de S.I. em padrões de segurança da informação internacionalmente aceitos, objetivando maximizar a abrangência dos aspectos culturais essenciais.

Considerando que cada organização forma sua própria cultura, pautada em certas práticas de segurança da informação usualmente seguidas e incorporadas no ambiente de trabalho (MARTINS e ELOFF, 2002), faz-se necessária a utilização de padrões que sejam comuns entre as organizações para que se possa avaliar a cultura de S.I. Nesta pesquisa se adotou como padrões aceitos os nove princípios de cultura de S.I. estabelecidos pela OCDE (2002), amplamente detalhados no tópico 2.6, e as normas da família ABNT NBR ISO/IEC 27000, que foram concebidas para todos os tipos e tamanhos de organizações (públicas e privadas, comerciais ou sem fins lucrativos) usarem como uma referência na implementação de controles de segurança da informação comumente aceitos.

Para a avaliação da cultura, o estudo referencia, também, a norma NBR ISO/IEC 27002 - Código de prática para controles de segurança da informação. A referida norma especifica a matriz de referência da avaliação, estruturada em 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles. Os objetivos de controle são as declarações do que se espera que seja alcançado na seção e o controle define a declaração específica para se atender o objetivo de controle e é detalhado por meio das Diretrizes para Implementação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b, p. 1).

Cada seção de controle contém um ou mais objetivos de controle e cada objetivo contém um ou mais controles. A figura 3 mostra o diagrama relacional entre os elementos da norma.

Figura 3 - Relacionamento dos elementos da norma 27002



Fonte: Próprio autor

As 14 seções e seus respectivos objetivos de controle estão relacionados a seguir:

1. Política de segurança da informação:
Orientação para direção para segurança da informação
2. Organização da segurança da informação:
Organização interna
Dispositivos móveis e trabalho remoto
3. Segurança em recursos humanos:
Antes da contratação
Durante a contratação
Encerramento e mudança da contratação
4. Gestão de ativos:
Responsabilidade pelos ativos
Classificação da informação
Tratamento de mídias
5. Controle de acesso:
Requisito do negócio para controle de acesso
Gerenciamento de acesso do usuário
Responsabilidades dos usuários

- Controle de acesso ao sistema e à aplicação
- 6. Criptografia:
 - Controles criptográficos
- 7. Segurança física e do ambiente
 - Áreas seguras
 - Equipamento
- 8. Segurança nas operações:
 - Responsabilidade e procedimentos operacionais
 - Proteção contra *malware*
 - Cópias de segurança
 - Registro e monitoramento
 - Controle de software operacional
 - Gestão de vulnerabilidades técnicas
 - Considerações quanto à autoria de sistemas da informação
- 9. Segurança nas comunicações:
 - Gerenciamento da segurança em redes
 - Transferência de informação
- 10. Aquisição, desenvolvimento e manutenção de sistemas:
 - Requisitos de segurança de sistemas de informação
 - Segurança em processos de desenvolvimento e de suporte
 - Dados para teste
- 11. Relacionamento na cadeia de suprimento:
 - Segurança da informação na cadeia de suprimento
 - Gerenciamento de entrada do serviço do fornecedor
- 12. Gestão de incidentes:
 - Gestão de incidentes de segurança da informação e melhorias
- 13. Aspectos da segurança da informação na gestão da continuidade do negócio:
 - Continuidade da segurança da informação
 - Redundância
- 14. Conformidade:

Conformidade com os registros legais e contratuais

Análise crítica da segurança da informação

Em síntese, este estudo fundamenta a avaliação da cultura organizacional de segurança da informação nos nove princípios da OCDE (2002) - Sensibilização, Responsabilidade, Resposta, Ética, Democracia, Avaliação de risco, Projeto de Segurança e Implementação, Gestão de Segurança e Reavaliação - e nos controles propostos pela norma NBR ISO/IEC 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b).

O instrumento de medida do nível de cultura organizacional de segurança da informação está respaldado na Teoria Psicométrica e na Teoria da Resposta ao Item - TRI.

2.8 TEORIA PSICOMÉTRICA

A Psicometria, campo da Psicologia, oferece a fundamentação teórica e epistemológica de medida para a representação numérica de fenômenos psicológicos (PASQUALI, 2009). Adotar os fundamentos da teoria psicométrica para a construção do instrumento de medida garante segurança no acesso às medidas dos fenômenos psicológicos, e consequentemente qualificam uma avaliação cientificamente respaldada (CRUZ e ALCHIERI, 2003).

De acordo com Cruz e Alchieri (2003), medir é aferir propriedades psicológicas com foco em um construto previamente delimitado. A "avaliação psicológica" dos fenômenos e processos psicológicos deve considerar três critérios interdependentes: a medida, o instrumento e o processo de avaliação.

Nesse sentido, a teoria psicométrica contribui no desenvolvimento do instrumento de avaliação da cultura organizacional de segurança da informação, objeto deste estudo que, na psicometria, é denominado traço latente ou construto. As estruturas latentes possuem atributos e estes atributos possuem magnitudes, ou seja, é possível mensurá-los e expressá-los por um conjunto de itens observáveis. A psicometria propõe os meios para a validação e identificação das evidências de confiabilidade das medidas desenvolvidas (PASQUALI, 1997).

O foco da pesquisa psicométrica é a demonstração da equivalência entre os processos empíricos (etapa de medida) e os processos teóricos (etapa de caracterização teórica) do traço latente. Essa demonstração é a validade do instrumento e a fidedignidade é a confiabilidade. Um instrumento adequado deve ser válido e fidedigno com o objeto de estudo (PASQUALI, 1997). A seguir, serão abordados os conceitos de traço latente, validade e fidedignidade.

2.8.1 Traço Latente

Para Pasquali (1997), o traço latente é uma variável hipotética de caráter matemático ou estatístico, ou seja, o fator ou o objeto de estudo que deve ser medido. Bortolotti (2010), considera o traço latente ou variável latente uma característica do indivíduo, empresa, município, etc, que não pode ser medida diretamente. Cada traço latente é composto por uma série de atributos que visam caracterizá-lo por um todo (PASQUALI, 1997).

Para o estudo, conforme visto, considera-se traço latente a cultura organizacional de segurança da informação e os seus atributos os princípios descritos no tópico 2.6 do capítulo 2, Princípios Diretivos de uma Cultura Organizacional de Segurança da Informação.

2.8.2 Validação

A validade de um teste é conferida quando ao se medir os itens que traduzem o traço latente verifica-se que se está medindo o próprio traço latente. A validação é a verificação empírica da hipótese (teoria). Um teste tem validade de conteúdo se ele possui uma amostra representativa de um universo finito de itens (PASQUALI, 1997).

2.8.3 Fidedignidade

A fidedignidade refere-se à confiabilidade do instrumento de medida. A fidedignidade de um teste está relacionada ao erro de medida produzido pelo próprio instrumento, ou seja, ao quanto o escore obtido no teste se aproxima do escore verdadeiro do sujeito, em um traço qualquer. Pode-se afirmar, então, que se trata da precisão ou calibração do instrumento de medida (PASQUALI, 1997).

2.9 TEORIA DA RESPOSTA AO ITEM

A Teoria da Resposta ao item, TRI, teoria da psicometria, teve suas origens nos anos 1930 e foi estruturada nos anos 1960. A TRI surgiu para resolver alguns problemas que a psicometria clássica, ou teoria clássica dos testes - TCT, apresentava, como a dependência do instrumento com o objeto medido e a preocupação com o teste como um todo, e não com os seus itens (PASQUALI e PRIMI, 2003). Assim, na TCT dois respondentes diferentes podem receber o mesmo escore, ainda que possuam proficiências ou aptidões diferentes, o que impossibilita a comparação entre os avaliados.

A TRI se refere a um conjunto de modelos matemáticos que relaciona as variáveis observáveis (itens do instrumento) aos traços hipotéticos não-observáveis (aptidões dos respondentes) (PASQUALI e PRIMI, 2003). A TRI leva em consideração os itens do teste como um todo, diferente da Teoria Clássica do Teste - TCT. Uma vez conhecido o escore (resultado do teste), é possível estimar as características dos respondentes (itens respondidos).

Com a utilização da TRI é possível estabelecer qualquer medição a partir de um conjunto de características do objeto de estudo que se pretende mensurar (VARGAS, 2007).

Andrade, Tavares *et al.* (2000, p. 7) ensinam que:

A TRI é um conjunto de modelos matemáticos que procuram representar a probabilidade de um indivíduo dar uma certa resposta a um item como função dos parâmetros do item e da habilidade (ou habilidades) do respondente. Essa relação é sempre expressa de tal forma que quanto maior a habilidade, maior a probabilidade de acerto no item.

Consoante a definição de Lord (1980) a Teoria da Resposta ao Item (TRI) é um conjunto de modelos probabilísticos que relaciona um traço latente de um respondente (Θ), com a probabilidade de este responder a um item dentro de uma determinada categoria. Considera-se traço latente ou variável latente uma característica do indivíduo que não pode ser medida diretamente (BORTOLOTTI, 2010).

Alguns autores referem-se ao traço latente com expressões tais como “variável hipotética, variável fonte, fator, construto, conceito, estrutura psíquica, traço cognitivo, processo cognitivo, processo mental, estrutura mental, habilidade, aptidão, traço de personalidade, processo elementar de informação, [...], atitude e outros.” (PASQUALI, 2004, p 55).

A principal distinção entre os modelos da TRI refere-se à seleção de opções de uma resposta, a relação entre os itens e o nível do traço latente. Com relação ao item, os modelos diferem quanto ao tipo de categoria de resposta, podendo ser itens dicotômicos (certo e errado ou concordo e discordo) ou itens politômicos (categorias graduais de respostas)(ANDRADE, TAVARES *et al.*, 2000; ARAUJO, ANDRADE *et al.*, 2009; MENEGON, 2013).

Dentre os modelos da TRI, o modelo proposto por Samejima (1969), Modelo de Resposta Gradual - MRG, é o que melhor atende aos requisitos do instrumento de medida deste estudo, pois trata-se de um modelo acumulativo, ou seja, a proficiência no nível mais alto contém o nível anterior. Outra característica do modelo é que ele trabalha com itens cujas repostas são graduadas. No MRG é possível extrair mais informações do item do que simplesmente se sua resposta está certa ou errada (ANDRADE, TAVARES *et al.*, 2000). Em um MRG, as respostas de um item são divididas em categorias politômicas e ordinais (SAMEJIMA, 1969).

O estudo apresenta, de forma resumida, o modelo de resposta gradual de Samejima, uma vez que se trata de um modelo clássico na literatura. Para maior aprofundamento sobre o tema, as seguintes referências podem ser consultadas: Andrade, Tavares *et al.* (2000), Baker (2001), Lord (1980) ou Samejima (1969).

O MRG de Samejima pode ser assim definido:

Seja a probabilidade de um indivíduo j escolher uma determinada categoria k , ou maior, no item i dada por:

$$P_{i,k}^+(\theta_j) = \frac{1}{1 + e^{-a_i(\theta_j - b_{i,k})}} \quad (1)$$

onde:

- i são os itens 1..I
- j os avaliados 1 ... n
- k categorias (0,1,2,3,4,...,m_i)
- θ o traço latente
- a_i o parâmetro de discriminação do item i
- $b_{i,k}$ o parâmetro de dificuldade associado a k -ésima categoria do item i

No MRG de Samejima são analisados dois parâmetros do item, a discriminação e a dificuldade (EMBRETSON, 2000).

A discriminação, parâmetro a , representa a capacidade do item de distinguir ou classificar o avaliado segundo um determinado traço latente, ou seja, o parâmetro a determina a qualidade do item. Quanto maior o seu valor, maior o seu poder de discriminação.

O parâmetro $b_{i,k}$ do item i , medido na mesma escala da habilidade θ , define o ponto na escala a partir do qual um avaliado apresenta uma alta probabilidade de responder a categoria k .

No MRG de Samejima a discriminação depende do parâmetro a (comum a todas as categorias) e dos parâmetros b adjacentes. Assim, existe uma ordenação das categorias de um determinado item segundo o seu nível de dificuldade b , ou seja, dado um item i tem-se (MENEGON, 2013):

$$b_{i,1} \leq b_{i,2} \leq b_{i,3} \dots \leq b_{i,m_i}$$

A probabilidade de um indivíduo j responder a uma determinada categoria k no item i é dada por:

$$P_{i,k}(\theta_j) = P_{i,k}^+(\theta_j) - P_{i,k+1}^+(\theta_j) \quad (2)$$

Por definição:

$$P_{i,0}^+(\theta_j) = 1 \quad (3)$$

e

$$P_{i,m_i+1}^+(\theta_j) = 0 \quad (4)$$

Aplicando as definições anteriores, obtém-se:

$$P_{i,k}(\theta_j) = \frac{1}{1+e^{-a_i(\theta_j-b_{i,k})}} - \frac{1}{1+e^{-a_i(\theta_j-b_{i,k+1})}} \quad (5)$$

Tem-se que a precisão de um instrumento de avaliação é medida pela totalidade das informações dos seus itens. Assim, a informação do item é definida como sendo o inverso da precisão com a qual seus parâmetros foram estimados (BAKER, 2001, p. 104)

A equação 6, abaixo, sintetiza esse conceito genérico, onde I é a quantidade de informação do item e σ^2 é a variância dos seus estimadores:

$$I = \frac{1}{\sigma^2} \quad (6)$$

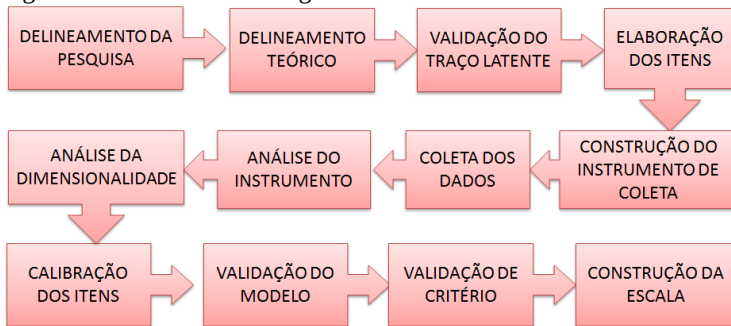
Um instrumento de avaliação (teste) é constituído por um conjunto de itens. Assim, a precisão do teste é dada pela somatória das quantidades de informação dos seus itens (BAKER, 2001).

$$I(\theta) = \sum_{i=1}^n I_i(\theta) \quad (7)$$

3 MÉTODO

O estudo proposto objetiva a elaboração de um instrumento de avaliação da cultura organizacional de segurança da informação e a construção de uma escala de medida. Este capítulo apresenta a descrição detalhada da metodologia utilizada para o desenvolvimento dos trabalhos, passando pelo delineamento da pesquisa à definição dos procedimentos aplicados na análise do instrumento de avaliação. A figura 4 sintetiza em forma de fluxo os passos da metodologia.

Figura 4 - Fluxo da metodologia



Fonte: Próprio autor

3.1 DELINEAMENTO DA PESQUISA

Para o delineamento da pesquisa se utiliza a classificação adotada pelos autores Silva e Menezes (2005) e Miguel, Fleury *et al.* (2012).

- **Do ponto de vista dos seus objetivos:** A pesquisa possui características descritiva e explicativa, uma vez que estuda o tema com fundamento nas teorias, conceitos e trabalhos existentes, aprofundando o conhecimento científico sobre o assunto, com aplicação prática.
- **Do ponto de vista de sua natureza:** A pesquisa é aplicada, pois busca apresentar um produto capaz de mensurar o nível da organizacional de segurança da informação.
- **Do ponto de vista da abordagem do problema:** A pesquisa é quantitativa na medida em que propõe a quantificação do traço latente (Cultura Organizacional

de Segurança da Informação) por meio da utilização de métodos estatísticos e da TRI. Não obstante, o estudo também apresenta uma abordagem qualitativa no processo de validação do traço latente e de interpretação da escala.

- **Do ponto de vista dos procedimentos técnicos:** A pesquisa é bibliográfica, tendo em vista que é elaborada com base em materiais científicos publicados. Também se classifica em pesquisa de levantamento (Survey) uma vez que será utilizado um questionário para a coleta dos dados necessários para a avaliação do objeto de pesquisa.

3.2 DELINEAMENTO TEÓRICO

A fundamentação teórica do estudo está focada na definição de cultura organizacional de segurança da informação.

Para tanto, o trabalho se apoia nas teorias das ciências sociais (Antropologia e Psicologia) para fundamentar o conceito de cultura organizacional, e nas ciências da Computação e da Informação e da Engenharia de Produção para subsidiar a avaliação do fator humano na segurança da informação nas organizações, inclusive aquelas pertencentes a uma cadeia de suprimentos, e, consequentemente, dar o suporte teórico para a consolidação da definição do traço latente (cultura organizacional de segurança da informação).

A elaboração dos itens do instrumento de avaliação se norteia em diretrizes e normas comumente aceitas na segurança da informação, para possibilitar a mensuração dos aspectos subjetivos da cultura com base em requisitos objetivos e comuns entre as organizações. Adotam-se as diretrizes da OCDE (2002) para uma cultura de S.I nas organizações e as normas da família ABNT NBR ISO/IEC 27000, que definem as orientações para uma segurança da informação adequada.

O estudo recorreu, também, à psicometria e à Teoria da Resposta ao Item – TRI., para respaldar a análise dos itens, a validação do instrumento de avaliação e, consequentemente, garantir a construção da escala do nível de cultura organizacional de S.I.

3.3 DEFINIÇÃO DO TRAÇO LATENTE

A fundamentação da conceituação da Cultura Organizacional de Segurança da Informação, traço latente objeto de avaliação, foi obtida por meio de ampla pesquisa bibliográfica em documentos técnicos e científicos (vide tabela 1 – Frequência da ocorrência das principais palavras-chaves aferidas nas bases de dados disponíveis). Esta etapa da pesquisa teve caráter qualitativo. As fontes de dados foram os artigos científicos publicados em revistas especializadas. O meio de busca mais utilizado foi o portal de serviços da Capes, no endereço <http://www.periodicos-capes.gov.br>. Por meio dele, foi possível acessar os principais indexadores científicos que, por sua vez, permitiu o acesso às bases de publicações pertinentes.

Foram utilizadas palavras-chaves previamente selecionadas relacionadas ao tema de pesquisa e acrescidas à medida que os levantamentos realizados eram ampliados (Segurança da Informação; Cultura Organizacional; Teoria da Resposta ao Item; Escala de Proficiência; Cadeia de Suprimentos). Quanto ao período de publicação dos artigos, priorizou-se o material mais atualizado e foram selecionados aqueles com maior contribuição e relevância para o estudo.

3.4 ELABORAÇÃO DOS ITENS

O Item consiste na unidade básica de um instrumento de coleta de dados, que pode ser uma prova, um questionário, etc.(BRASIL, 2006).

Segundo Baker (2001), cada item deve medir uma única faceta (um aspecto particular do traço latente), e prover as condições necessárias para que o avaliado possa escolher a resposta que lhe é mais adequada.

A elaboração dos itens para compor o instrumento de avaliação foi fundamentada nos princípios definidos pela OCDE (2002), tópico 2.6, e nas normas da família ABNT NBR ISO/IEC 27000, em especial na norma NBR ISO/IEC 27002, que estabelece os controles que devem ser implementados para uma segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b, p. 1).

Nesse sentido, o processo de elaboração dos itens teve como pré-requisito a definição de uma matriz de referência conten-

do todas as descrições e definições de cada faceta pesquisada. A partir de agora, para efeitos de compatibilidade com a TRI, os princípios da cultura organizacional de segurança da informação passam a se chamar de facetas.

A matriz de referência foi dividida em nove agrupamentos sendo um para cada princípio que compõe o traço latente (Sensibilização ou Consciência, Responsabilidade, Resposta ou Reação, Ética, Democracia, Projeto de Segurança e Implementação, Gestão de Segurança e Reavaliação) (OCDE, 2002).

O quadro 1 apresenta a matriz de referência com a definição e a descrição de cada faceta (princípio) do traço latente. A definição e a descrição da faceta contemplam as orientações e os requisitos que devem ser atendidos na elaboração dos itens que compõem o instrumento de avaliação.

Quadro 1 - Matriz de Referência

Faceta	Consciência
Definição	As partes interessadas devem estar cientes da necessidade de garantir a segurança dos sistemas de informação e de redes, e do que elas podem fazer para melhorar a segurança.
Descrição	- Os participantes devem entender que as falhas na segurança podem prejudicar significativamente os sistemas e redes sob seu controle, bem como os dos outros. - Os participantes devem, também, ter conhecimento da configuração e das atualizações disponíveis para seus sistemas, do lugar que ocupam nas redes e das boas práticas que possam implementar para melhorar a segurança. - Os participantes devem considerar as necessidades dos outros participantes.
Faceta	Responsabilidade
Definição	Todos os participantes são responsáveis pela segurança dos sistemas de informação e de redes
Descrição	- Eles devem compreender a sua responsabilidade pela segurança desses sistemas e redes. - Devem prestar contas, na razão de suas funções individuais. - Os participantes devem, regularmente, rever e avaliar suas próprias políticas, práticas, medidas e procedimentos para se assegurarem que estão adequados ao seu ambiente. - Os participantes devem considerar a segurança dos sistemas e redes e divulgar as informações adequadas, incluindo atualizações em tempo hábil
Faceta	Resposta (reação)
Definição	Os participantes devem agir em tempo hábil e de maneira cooperativa para prevenir, detectar e responder a incidentes de segurança.
Descrição	- Os participantes devem reagir prontamente e com um espírito de cooperação aos incidentes de segurança - Devem compartilhar suas informações sobre ameaças e vulnerabilidades - Devem implementar procedimentos para a rápida e

	efetiva cooperação a fim de prevenir, detectar e responder a incidentes de segurança
Faceta	Ética
Definição	Os participantes devem respeitar os interesses legítimos de outros participantes.
Descrição	- Os participantes devem reconhecer o quanto suas ações ou omissões podem prejudicar os outros. - Devem ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação. - Devem respeitar os interesses legítimos dos outros participantes.
Faceta	Gestão de segurança
Definição	Os participantes devem adotar uma abordagem abrangente para a gestão da segurança.
Descrição	- Deve ser baseada na avaliação dos riscos. - Deve ser dinâmica e global, de modo a abranger todos os níveis de atividades dos participantes e todos os aspectos de suas operações. - Deve incluir, respostas antecipadas às ameaças emergentes e a prevenção, detecção e resolução dos incidentes, a recuperação dos sistemas, a manutenção contínua, o controle e a auditoria. - As políticas de segurança dos sistemas e redes de informações, as práticas, medidas e procedimentos em matéria de segurança devem ser coordenados e integrados para criar um sistema coerente de segurança. - Os requisitos da gestão de segurança dependem do nível de envolvimento, do papel do participante, dos riscos envolvidos e das características do sistema.
Faceta	Democracia
Definição	A segurança dos sistemas e redes de informação deve ser compatível com os valores essenciais de uma sociedade democrática.

Descrição	- Os participantes devem respeitar os valores, a liberdade de troca de ideias, pensamentos, o livre fluxo de informações, a confidencialidade da informação e da comunicação, a proteção adequada dos dados pessoais, a abertura e a transparência. - Os participantes devem respeitar e reconhecer a liderança.
Faceta	Avaliação de risco
Definição	Os participantes devem realizar avaliações de risco.
Descrição	- As avaliações devem ser suficientemente amplas para abranger o conjunto dos principais fatores internos e externos, tais como tecnologia, fatores físicos e humanos, políticas e serviços de terceiros que influenciam na segurança da informação.
Faceta	Projeto de segurança e implementação
Definição	Os participantes devem integrar a segurança como um elemento essencial dos sistemas e redes de informação.
Descrição	- Os participantes devem preocupar-se com a criação e adoção de salvaguardas e soluções para evitar ou limitar o dano potencial de ameaças e vulnerabilidades identificadas.
Faceta	Reavaliação
Definição	Os participantes devem analisar e reavaliar a segurança dos sistemas e redes de informação, e fazer as modificações necessárias nas políticas, práticas, medidas e procedimentos de segurança.
Descrição	- Todos os participantes devem continuamente rever, reavaliar e modificar todos os aspectos da segurança para lidar com esses riscos que estão em evolução.

Fonte: OCDE, 2002; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b.

Uma vez definida a matriz de referência, o processo de elaboração dos itens aconteceu em duas etapas. A primeira etapa foi a de redação de itens que atendessem aos requisitos definidos na matriz de referência. Tendo encerrado essa fase, os itens foram apresentados a uma banca de juízes (especialistas) para avaliação e proposta de alteração, se fosse o caso, a fim de adequação à

realidade das organizações (para maior descrição acerca dos juízes vide tópico 3.7.5).

Esse processo resultou na definição de 150 itens de avaliação cobrindo as nove facetas e satisfazendo os requisitos dos 22 descritores da matriz de referência. A relação completa de todos os itens e as suas respectivas justificativas pode ser encontrada no apêndice A.

Os itens desenvolvidos são do tipo politômico. A escolha do tipo de item relaciona-se à natureza e às características do traço latente - cultura organizacional de segurança da informação. O item do tipo politômico permite obter, dos respondentes, o grau, a intensidade ou a frequência com que ele atende ao questionamento. A escala gradual adotada nos itens pode conter de 2 a 4 categorias, dependendo do que está sendo avaliado.

A constituição dos itens de avaliação é composta por duas partes: a primeira é chamada de contextualização. Nessa parte do item, descreve-se uma situação-problema de modo a criar um cenário para o avaliado responder ao item. A segunda parte é o questionamento propriamente dito.

O quadro 2 exemplifica a estrutura de um item. Nesse caso, trata-se de item da faceta Consciência contendo quatro categorias.

Quadro 2 - Exemplo da constituição de um item

Csc_01_0	Os "malwares" são programas que causam danos aos sistemas computadorizados, como destruição e/ou roubo de dados.	Nunca	Raramente	Frequentemente	Sempre	N.A.*
Csc_01_1	Com que frequência você verifica se o antivírus está atualizado?					
Csc_01_2	Com que frequência você verifica o histórico (Relatório) do antivírus?					

* Não se Aplica

3.5 CONSTRUÇÃO DO INSTRUMENTO DE COLETA

Como relatado anteriormente, a quantidade de itens elaborados para cobrir todas as facetas atingiram um valor que tornou inviável a aplicação de um único questionário contendo todos os itens a um mesmo respondente. Assim, a solução foi a utilização

de Blocos Incompletos Balanceados- BIB. O problema é que a adoção de BIB resulta em um número grande de cadernos (questionários) que eleva muito o número de respondentes. Por esse motivo, foi necessária a adoção do delineamento de PBIB – Blocos Incompletos Parcialmente Balanceados que, dado as suas características, permite a construção de um número menor de cadernos.

A construção do instrumento de coleta na forma proposta objetivou evitar o cansaço ou desistência do respondente. Assim, os itens foram distribuídos em 10 blocos de 15 itens cada. A condição para a distribuição dos itens nos blocos foi que cada um dos blocos contemplasse itens das nove facetas, para que cada respondente fosse exposto ao máximo de facetas. Após a construção dos blocos foram montados 10 cadernos. Cada caderno com 2 blocos, totalizando 30 itens por caderno. Esse procedimento permitiu que cada bloco de itens fosse respondido em dois cadernos, criando uma ligação entre os cadernos por meio dos blocos em comum. Por exemplo, o caderno 1 se liga ao caderno 2 por meio do bloco 2, e assim por diante.

O quadro 3 a seguir retrata a distribuição dos itens nos blocos e cadernos.

Quadro 3 - Composição dos blocos e cadernos

	Caderno 1		Caderno 3		Caderno 5		Caderno 7		Caderno 9		
	Bloco 1	Bloco 2	Bloco 3	Bloco 4	Bloco 5	Bloco 6	Bloco 7	Bloco 8	Bloco 9	Bloco 10	Bloco 1
1	Csc. 01.1	Csc. 01.2	Csc. 02.1	Csc. 02.2	Csc. 02.3	Csc. 03.1	Csc. 03.2	Csc. 03.3	Csc. 03.4	Csc. 03.5	Csc. 01.1
2	Csc. 03.6	Csc. 03.7	Csc. 04.1	Csc. 04.2	Csc. 04.3	Csc. 05.1	Csc. 05.2	Csc. 05.3	Csc. 05.4	Rsp. 01.1	Csc. 03.6
3	Rsp. 02.1	Rsp. 02.2	Rsp. 02.3	Rsp. 03.1	Rsp. 03.2	Rpt. 01.1	Rpt. 01.2	Rpt. 01.3	Rpt. 01.4	Rpt. 02.1	Rsp. 02.1
4	Rpt. 02.2	Rpt. 02.3	Rpt. 02.4	Rpt. 03.1	Rpt. 03.2	Rpt. 03.3	Rpt. 04.1	Rpt. 04.2	Etc. 01.1	Etc. 01.2	Rpt. 02.2
5	Etc. 01.3	Etc. 01.4	Etc. 01.5	Etc. 01.6	Etc. 01.7	Etc. 01.8	Etc. 02.1	Etc. 02.2	Etc. 03.1	Etc. 03.2	Etc. 01.3
6	Etc. 03.3	Etc. 03.4	Etc. 04.1	Etc. 04.2	Etc. 05.1	Etc. 05.2	Etc. 05.3	Etc. 05.4	Etc. 06.1	Etc. 06.2	Etc. 03.3
7	Etc. 06.3	Etc. 06.4	Gts. 01.1	Gts. 01.2	Gts. 01.3	Gts. 01.4	Gts. 01.5	Gts. 01.6	Gts. 02.1	Gts. 02.2	Etc. 06.3
8	Dmc. 01.1	Dmc. 01.2	Dmc. 01.3	Dmc. 02.1	Dmc. 02.2	Dmc. 02.3	Dmc. 03.1	Dmc. 03.2	Dmc. 03.3	Dmc. 04.1	Dmc. 01.1
9	Dmc. 04.2	Dmc. 05.1	Dmc. 05.2	Dmc. 06.1	Dmc. 06.2	Dmc. 06.3	Rsc. 01.1	Rsc. 01.2	Rsc. 01.3	Rsc. 02.1	Dmc. 04.2
10	Rsc. 02.2	Rsc. 03.1	Rsc. 03.2	Rsc. 03.3	Rsc. 04.1	Rsc. 04.2	Rsc. 04.3	Rsc. 05.1	Rsc. 05.2	Rsc. 05.3	Rsc. 02.2
11	Rsc. 06.1	Rsc. 06.2	Rsc. 06.3	Rsc. 07.1	Rsc. 07.2	Rsc. 07.3	Rsc. 08.1	Rsc. 09.1	Rsc. 09.2	Rsc. 09.3	Rsc. 06.1
12	Rsc. 09.5	Rsc. 10.1	Rsc. 10.2	Rsc. 11.1	Rsc. 11.2	Rsc. 11.3	Rsc. 11.4	Rsc. 12.1	Rsc. 12.2	Rsc. 12.3	Rsc. 09.5
13	Rsc. 12.4	Rsc. 12.5	Rsc. 12.6	Rsc. 17.1	Rsc. 17.2	Rsc. 13.1	Rsc. 13.2	Rsc. 14.1	Rsc. 14.2	Rsc. 14.3	Rsc. 12.4
14	Rsc. 15.1	Rsc. 15.2	Rvl. 01.1	Rvl. 02.1	Rvl. 02.2	Rvl. 02.3	Rvl. 01.1	Rvl. 01.2	Rvl. 02.1	Rvl. 02.2	Rsc. 15.1
15	Rvl. 02.3	Rsc. 09.4	Rsc. 16.1	Rsc. 16.2	Rsc. 16.3	Rsc. 16.4	Rsc. 12.9	Rsc. 08.2	Rsc. 08.3	Csc. 06.1	Rvl. 02.3
	Caderno 2		Caderno 4		Caderno 6		Caderno 8		Caderno 10		

Fonte: Próprio autor

Além dos 30 itens dos cadernos, foi inserido um item comum a todos os cadernos que é um item de autoavaliação:

"Como você avalia o seu conhecimento sobre o tema segurança da informação?"

Respostas: Não tenho conhecimento; Tenho um conhecimento superficial; Tenho um conhecimento mediano; Tenho domínio sobre o tema.

O objetivo desse item é fazer com que o respondente faça uma autoavaliação sobre o tema. Esse item será utilizado posteriormente para subsidiar a validação de critério.

3.6 COLETA DE DADOS

Os dados necessários para a construção da escala são provenientes dos colaboradores das organizações participantes da pesquisa. Por esse motivo, a coleta de dados obedeceu rigorosamente às normas do comitê de ética estabelecidas na resolução CNS 466/2012, cujo projeto foi registrado e aprovado sob o protocolo CAAE 61718116.5.0000.

O processo de inclusão das organizações na pesquisa ocorreu em duas etapas. Na primeira, foram escolhidas organizações que, a princípio, teriam pouca, média e alta proficiência em segurança da informação, por meio de pesquisa em sites do governo ou por indicação de especialistas.

A segunda etapa de eleição das organizações participantes consistiu na realização de entrevistas com os responsáveis pelas organizações escolhidas na etapa anterior, ou com o representante por ele indicado. Foram feitas aproximadamente 30 reuniões, presenciais e por videoconferência. Durante as reuniões foram apresentados aos gestores todos os aspectos da pesquisa, desde sua concepção, metodologia, apresentação prévia dos itens e sistema de coleta e procedimentos de confidencialidade dos respondentes e das organizações.

Após a etapa de entrevistas, foram selecionadas quinze organizações públicas, da administração direta, autarquias, fundações e empresas públicas do Poder Executivo e do Poder Judiciário. Das quinze organizações selecionadas, apenas sete confirmaram sua participação, as demais desistiram, devido a problemas conjunturais ocasionados pelo momento político, já em um momento avançado no cronograma da pesquisa, o que impossibilitou a inclusão de novas organizações.

As organizações que fizeram parte da pesquisa estão espalhadas pelo território nacional, deste modo, optou-se por utilizar a Internet para fazer a coleta de dados. Para tanto foi desenvolvido

um sistema para captar os dados e controlar a distribuição dos questionários de forma a garantir que fossem distribuídos igualmente entre os respondentes.

O sistema ficou hospedado nos servidores da UFSC, sendo o seu acesso por meio do protocolo HTTPS para garantir a segurança do respondente.

As organizações participantes impuseram duas condições: a não identificação dos colaboradores e das organizações, e a comunicação/convocação para responder aos questionários seria de exclusiva responsabilidade da organização. Essas condições, que foram atendidas, não permitiram o planejamento de uma amostra que fosse representativa a nível das organizações.

O processo de coleta de dados tem início com o aceite da organização em participar da pesquisa. A organização, por sua vez, assina uma declaração informando estar ciente dos procedimentos de coleta de dados. Em seguida, a organização informa os seus dados para a composição do cadastro, tais como: Nome da organização, responsável, número de colaboradores, etc.

O passo seguinte foi a aplicação dos questionários junto aos colaboradores. Esse passo tem início na instância mais elevada da organização, ou por uma pessoa por ela designada para acompanhar a pesquisa. O responsável, por sua vez, faz uma chamada ou uma convocação junto aos colaboradores, por meio do(s) sistema(s) interno(s) de comunicação da organização. No comunicado é informada ao colaborador a importância da pesquisa para a organização, as instruções de preenchimento e o link de acesso ao questionário.

Cada colaborador que participa da pesquisa responde primeiro o documento Termo de Concordância, onde ele manifesta estar de acordo em participar. Caso o colaborador não concorde, o sistema simplesmente computa a desistência para fins de controles futuros.

3.7 PROCEDIMENTOS PARA ANÁLISE DO INSTRUMENTO

Essa etapa consiste na descrição dos procedimentos que permitem avaliar as características do instrumento de coleta dos dados, a sua consistência, dimensionalidade e independência

local. Com relação aos itens, os procedimentos referem-se à avaliação da qualidade e calibração.

3.7.1 Consistência dos cadernos

Esta etapa é a mais importante, pois, dela depende toda a qualidade da pesquisa.

Embora o sistema construído para a coleta de dados possua procedimentos de análise de consistência em tempo real para evitar cadernos incompletos, distribuição inadequada e preenchimento não identificado ou não autorizado, julgou-se necessária a realização de mais dois procedimentos de crítica para detectar possíveis problemas não previstos ou não controláveis que pudessem ter ocorrido durante o procedimento da coleta de dados:

- Retirada dos cadernos que apresentam respostas sistemáticas ou tendenciosas, como por exemplo, respondentes que selecionam só uma coluna de resposta; e
- Retirada dos cadernos com tempo de preenchimento incompatível com o comportamento médio dos respondentes.

3.7.2 Consistência dos itens

Após os procedimentos de análise da consistência dos questionários, é necessário analisar a consistência dos itens do instrumento.

O objetivo do processo é a identificação de itens que possam apresentar problemas quanto ao seu preenchimento, número de respostas insuficiente, itens sem respostas e itens com apenas um tipo de resposta. Trata-se de uma análise da frequência de resposta das categorias dos itens para observar o comportamento de resposta em cada item, pois a baixa frequência de resposta nas categorias do item ocasiona imprecisão/distorção na estimação dos seus parâmetros.

Os itens identificados nas inconsistências relacionadas são retirados da base ou têm suas categorias reagrupadas a fim de aproveitamento do item.

3.7.3 Dimensionalidade do Instrumento

Uma vez que o objetivo desse estudo é a criação de uma escala do nível de cultura organizacional de segurança da infor-

mação, faz-se necessária a verificação da dimensionalidade do instrumento.

Um instrumento de medida pode assumir duas situações distintas. Ele pode ser unidimensional ou multidimensional. A dimensionalidade é definida pela quantidade de fatores. Ou seja, um instrumento é considerado unidimensional se existir um único fator que explica o traço latente. O número de fatores, por sua vez, é obtido por meio da análise fatorial (TEZZA, 2012).

Devido às características da base de dados que foi constituída utilizando-se o delineamento PBIB, não foi possível utilizar as ferramentas de análise fatorial linear ou de correlação policórica, pois tais ferramentas necessitam que todos os itens sejam pareados, ou relacionados par-a-par, o que não ocorre quando se utiliza PBIB. Assim, para a determinação do número de dimensões do instrumento de avaliação foi utilizada a análise fatorial de informação completa, *full-information*. Trata-se de uma análise fatorial mais sensível e informativa para o processo de determinação da dimensionalidade do instrumento, uma vez que essa metodologia não utiliza a matriz de correlação ou covariância (BOCK, GIBBONS *et al.*, 1988; EMBRETSON, 2000).

O critério utilizado para identificar a pertinência do item com o fator foi sugerido por Hair, Black *et al.* (2009) e Pasquali (2009), que estabelece as diretrizes para identificação de cargas fatoriais significantes com base em tamanho de amostra. Para uma amostra $n > 350$ a carga fatorial do item para pertencer ao fator deve ser $\geq 0,30$ e sua comunalidade $\geq 0,20$.

Para a verificação da dimensionalidade pela análise fatorial de informação completa foi utilizado o pacote *MIRT* do *R*. Esse pacote contém todas as rotinas necessárias para a análise (CHALMERS, 2012).

3.7.4 Independência local

A independência local ou independência condicional é um dos pressupostos necessários para garantir o processo de estimação dos parâmetros do modelo. A independência local significa que os parâmetros de um item não são influenciados por outros itens, ou seja, a probabilidade de responder um item é estritamente determinada pelo nível do traço latente do respondente.

(LORD, 1980; ANDRADE, TAVARES *et al.*, 2000; BORTOLOTTI, 2010).

Conforme Hambleton, Swaminathan *et al.* (1991) a independência local é tida como uma consequência direta da unidimensionalidade do instrumento e do modelo. Se o instrumento for unidimensional, a independência local fica garantida, uma vez que existe uma única suposição a ser verificada (ANDRADE, TAVARES *et al.*, 2000; BARROS, 2016).

3.7.5 Avaliação da qualidade dos itens

O processo de avaliação da qualidade dos itens foi dividido em três momentos. O primeiro ocorreu ainda na fase de elaboração dos itens, onde todos os itens foram submetidos a uma banca de juízes para validar se os itens elaborados atendiam ao propósito da pesquisa. A banca de juízes foi constituída por profissionais especializados nas normas ABNT e OCDE e em segurança da informação, sendo: um Doutor em psicometria e quatro Mestres nas áreas de ciência da computação e do direito.

O segundo momento ocorre durante o processo de calibração dos itens. Nesse momento, identificam-se os itens que apresentam parâmetros que não atendem aos requisitos de qualidade descritos pela TRI (discriminação e dificuldade). O processo de calibração é detalhado no próximo tópico.

No terceiro momento de avaliação da qualidade dos itens, o instrumento, agora com os itens calibrados, é novamente apresentado à banca de especialistas, para referendar os resultados com o esperado empiricamente.

3.7.6 Calibração dos itens

O processo de calibração é o mais importante da TRI. É por meio da calibração que se estimam os parâmetros dos itens e as habilidades dos respondentes. As estimativas dos parâmetros dos itens obtidas fornecem as informações sobre as propriedades técnicas e psicométricas dos itens do teste (ANDRADE, TAVARES *et al.*, 2000; BAKER, 2001). Assim, durante o processo de calibração foi realizada a análise da qualidade do item com base nos parâmetros de discriminação e na magnitude dos erros padrões da estimativa dos parâmetros dos itens.

Para o processo de calibração foi utilizado uma ‘priori’, ou seja, uma restrição para o parâmetro ‘ α ’ que, no caso específico, é uma distribuição log-normal com média 0 e desvio padrão 0,5. O uso da ‘priori’ garante que a função estime parâmetros positivos para o ‘ α ’.

3.8 VALIDAÇÃO DO MODELO

Nas aplicações da TRI, a avaliação do ajuste do modelo é uma questão crítica (LI CAI e MARKATOS, 2013). “Um modelo é uma representação simplificada de algum problema ou situação da vida real destinado a ilustrar certos aspectos do problema sem se ater a todos os detalhes” (EMILIANO, VEIGA *et al.*, 2010, p. 1).

O procedimento de validação do modelo visa verificar a coerência do instrumento, ou o quanto o modelo está ajustado. Dentre os métodos de avaliação de um modelo, optou-se por adotar o índice *goodness-of-fit* composto pelas estatísticas RMSEARoot (*Mean Square Error of Approximation*) - Erro Quadrático Médio Aproximado, CFI (*Close Fit*) e TLI (*Tucker–Lewis index*). A razão da adoção dessas estatísticas se fundamenta no fato delas, praticamente, não serem sensíveis ao tamanho da amostra (BROWN, 2015).

Segundo Brown (2015, p. 74), os critérios que determinam a boa qualidade do modelo devem atender, no mínimo, a estatística $RMSEA < 0,05$ e as estatísticas CFI e TLI $> 0,90$.

No pacote *MIRT* do *R*, essas estatísticas são calculadas por meio da função *M2*.

3.9 VALIDAÇÃO DE CRITÉRIO

Essa validação visa verificar se o modelo está realmente medindo o traço latente - cultura organizacional de segurança da informação.

Para essa avaliação foram utilizados dois procedimentos. O primeiro, descrito a seguir, é um procedimento estatístico e o segundo, uma análise junto aos especialistas.

A validação estatística consiste em comparar os resultados obtidos por meio da utilização do modelo com resultados provenientes das respostas dos respondentes ao questionamento sobre sua autoavaliação no tema da segurança da informação. O

item "*autoaval - Como você avalia o seu conhecimento sobre o tema?*" recebe os resultados ordinais de 0 a 3, sendo: 0 - Não tenho conhecimento; 1 - Tenho um conhecimento superficial; 2 - Tenho um conhecimento mediano e 3 - Tenho domínio sobre o tema.

Para o teste, os escores dos respondentes foram categorizados para torná-los qualitativos. Em seguida, foi feita uma correlação entre os resultados do item autoavaliação e o escore para verificar a validação de critério.

O segundo procedimento consiste na apresentação dos resultados aos especialistas para que atestem se a escala desenvolvida efetivamente avalia o traço latente - cultura organizacional de segurança da informação.

3.10 CONSTRUÇÃO DA ESCALA

Uma vez que o modelo foi considerado ajustado, os parâmetros dos itens e as habilidades dos respondentes estão numa mesma métrica. Assim, têm-se as condições necessárias e suficientes para a construção de uma escala do nível da cultura organizacional de segurança da informação.

Este processo baseia-se na identificação dos níveis âncora e itens âncora. Segundo Andrade, Tavares *et al.* (2000) e (BEATON e ALLEN, 1992), níveis âncora são um conjunto de itens âncora, passíveis de serem interpretados na escala.

Sem uma escala, a única conclusão que se poderia chegar ao analisar os resultados é que uma organização que teve um escore de 1,0 é melhor que outra com escore 0,5, mas não é possível identificar o(s) motivo(s) da diferença, os pontos fortes e fracos das organizações em relação ao que se está avaliando.

A construção da escala tem início com o estabelecimento de valor de referência (uma origem e uma unidade de medida). Por definição, o valor de referência é o padrão (0,1), ou seja, média 0 e desvio padrão 1 (ANDRADE, TAVARES *et al.*, 2000).

Embora esses valores sejam padronizados, a sua interpretação pode não ser bem aceita pelo avaliado, pois uma organização que está abaixo da média teria um escore negativo, o que, a princípio, geraria uma conotação pejorativa.

Para contornar tal situação, é realizada uma transformação linear, fundamentada no princípio de invariância da TRI, para

estabelecer um referencial mais adequado, com escores positivos e, conseqüentemente, mais fácil de serem interpretados por pessoas “leigas”. Adotou-se o padrão (100,10), ou seja, média 100 e desvio padrão 10.

Função de transformação do escore (0,1) para (100,10).

$$\theta^* = \frac{\theta - \bar{\theta}}{\sigma} \sigma^* + \bar{\theta}^* \quad (8)$$

onde:

θ = escore no padrão(0,1)

$\bar{\theta}$ = Média dos escores(0,1) = 0,00048

σ = Desvio padrão dos escores(0,1) = 0,8939

θ^* = Novo escore Padrão (100,10)

σ^* = Novo Desvio Padrão = 10

$\bar{\theta}^*$ = Novamédia = 100

Constantes de transformação

$$\alpha^* = \frac{\sigma^*}{\sigma} \quad (9)$$

$$\beta^* = \beta - \alpha^* \bar{\theta} \quad (10)$$

Aplicando-se a esse caso, tem-se:

$$\alpha = 10$$

$$\beta = 100$$

$$\alpha^* = \frac{10}{0,8939} = 11,18693$$

$$\beta^* = 100 - 11,18693 * 0,00048 = 100,0054$$

A tabela 14 do apêndice D contém os novos valores dos parâmetros após a transformação.

A partir deste ponto, todas as análises têm como referência a escala (100,10).

Uma vez concluída a transformação, dá-se início a etapa de posicionamento dos itens. O processo de posicionamento consiste em determinar a posição do item por meio da probabilidade do respondente escolher uma determinada categoria. O critério utilizado para determinação do posicionamento da categoria do item foi $p(x = 1) \geq 0,6$, ou seja, no nível da escala a partir do qual

a probabilidade do respondente escolher uma determinada categoria deve ser maior ou igual a 0,6.

Ainda, se um item atender à condição $p(x = 1) \geq 0,6$ e o seu parâmetro de discriminação $\geq 1,0$, trata-se de item âncora.

4 ANÁLISE DOS RESULTADOS E DISCUSSÃO

Neste capítulo são apresentados os resultados obtidos nos procedimentos descritos no capítulo anterior e uma discussão sobre eles.

4.1 COLETA DE DADOS

O período de aplicação dos questionários junto à população da pesquisa (vide 3.6) foi de agosto de 2016 a maio de 2017.

A tabela 1 a seguir mostra o panorama da coleta de dados. Devido ao acordo de confidencialidade estabelecido com as organizações participantes, suas identificações foram preservadas.

Tabela 1 - Totalização da Coleta por Organização

ORGANIZAÇÃO	CONVOCADOS ¹	ACESSOS	DESISTÊNCIAS	TOTAL	APROVEITAMENTO %
1	80	33	12	21	26,25%
2	150	48	5	43	28,67%
3	150	67	12	55	36,67%
4	500	394	70	324	64,80%
5	1000	271	52	219	21,90%
6	2000	602	162	440	22,00%
7	200	40	8	32	16,00%
TOTAL	5080	1455	321	1134	30,9%

¹ o número de convocados foi informado pelas respectivas organizações

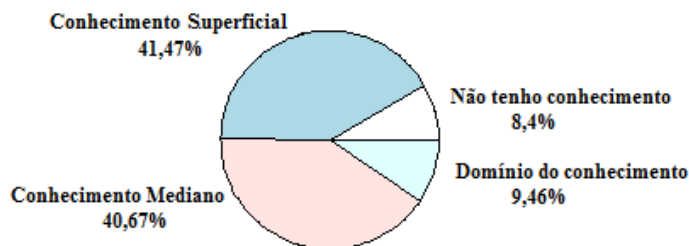
Fonte: Próprio autor

Em média 31% dos colaboradores convocados atenderam à pesquisa.

Considerando que o percentual de aproveitamento reflete a influência dos dirigentes nos seus colaboradores, a organização 4 demonstra que o seu dirigente exerce uma influência/liderança significativa junto aos seus colaboradores. A organização 4 possui regimento interno regrando que o dirigente pertença ao quadro da organização. Talvez seja esse o motivo do índice de aproveitamento ser o mais elevado dentre as organizações participantes.

A população que respondeu ao questionário se autoavaliou quanto ao seu conhecimento sobre segurança da informação. Aproximadamente 49,7% declararam ter pouco ou nenhum conhecimento sobre o tema, enquanto 50,3% possuem um conhecimento mediano ou domínio sobre segurança da informação.

Figura 5 - Distribuição por categoria de resposta



Fonte: Próprio autor

A tabela 2 a seguir apresenta a consolidação do resultado sobre a autoavaliação em nível de organização.

Tabela 2 - Como você avalia o seu conhecimento sobre o tema?

Organi- zação	Não tem conhe- cimento	Conhecimento superficial	Conhecimento mediano	Tem domínio
1	20,00%	40,00%	35,00%	5,00%
2	9,76%	48,78%	41,46%	0,00%
3	7,55%	43,40%	47,17%	1,89%
4	11,88%	46,56%	35,31%	6,25%
5	1,38%	21,56%	54,13%	22,94%
6	8,29%	46,77%	37,56%	7,37%
7	9,68%	41,94%	41,94%	6,45%
Média	8,24%	41,45%	40,82%	9,49%

Fonte: Próprio autor

A organização 5 se destaca, pois é a que possui o maior número de respondentes com o nível mais alto de conhecimento sobre segurança da informação. Trata-se de uma organização que, historicamente, vem desenvolvendo, há alguns anos, o processo de aculturação em segurança da informação.

Considerando o procedimento adotado para a coleta de dados, que atendeu às condições impostas pelas organizações participantes, verificou-se que a amostra de respondentes da organização ficou composta de voluntários. Como o objetivo da pesquisa é a construção de uma escala de medida, a amostra não comprometeu o estudo, pois se mostrou representativa e suficiente para a construção da escala.

4.2 ANÁLISE DO INSTRUMENTO

4.2.1 Análise de consistência dos cadernos

Havia-se previsto, no planejamento da pesquisa, uma análise visual de todos os cadernos em busca de respostas sistemáticas ou tendenciosas. No entanto, para auxiliar a análise visual devido ao elevado número de cadernos, verificou-se a necessidade de desenvolver um aplicativo que apresentasse as respostas no formato do caderno. A visualização nesse formato facilitou a detecção de padrões de resposta. Observou-se que os cadernos que apresentavam problemas de preenchimento tinham um tempo de preenchimento inferior a 3 minutos.

Diante da constatação anterior, foi feito um levantamento estatístico sobre o tempo de preenchimento dos cadernos. Os resultados estão descritos nas tabelas 3 e 4.

Tabela 3 - Tempo gasto no preenchimento em minutos

TEMPO MÉDIO	12,40
DESVIO PADRÃO	59,34
MEDIANA	7,00
TEMPO MÍNIMO	0,96
TEMPO MÁXIMO	1366,00

Fonte: Próprio autor

Tabela 4 - Frequência de preenchimento

Intervalo em minutos	Frequência
(00,03]	17
(03,05]	268
(05,10]	619
(10,20]	167
(20,30]	33
(30,40]	7
(40,50]	6
(≥ 50)	17
Total	1.134

Fonte: Próprio autor

A análise de consistência resultou na constatação de que os cadernos com respostas sistemáticas ou tendenciosas coincidem com aqueles com tempo de preenchimento incompatível (≤ 3 minutos). Assim, foram observados os dois requisitos de consistência dos cadernos descritos no tópico 3.7.1.

O processo de crítica eliminou 17 cadernos do arquivo.

Os cadernos que tiveram o seu tempo de preenchimento maior ou igual a 50 minutos foram mantidos, pois não apresentaram problemas em suas respostas. Isso ocorreu devido a orientação de preenchimento que “*em caso de cansaço ou necessidade, suspender o preenchimento e dar continuidade posteriormente*”.

A tabela 5 apresenta a frequência dos cadernos, após a eliminação dos cadernos inconsistentes.

Tabela 5 - Frequência por caderno

Caderno	Preenchidos	Tempo ≤ 3	Total líquido
1	108	3	105
2	109	1	108
3	116	1	115
4	111	0	111
5	117	1	116
6	120	1	119
7	114	3	114
8	114	5	109
9	112	2	110
10	113	0	113
Total	1.134	17	1.117

Fonte: Próprio autor

A princípio, buscou-se a obtenção de quantidades iguais de respondentes entre os cadernos. A variação do número de cadernos preenchidos observada foi ocasionada pelo resultado da análise acima descrita e pelas desistências no preenchimento, contabilizadas pelo sistema (consistência em tempo real).

Concluiu-se, portanto, pela consistência dos cadernos.

4.2.2 Análise de consistência dos itens

Verificada a consistência dos cadernos, passa-se a análise de consistência dos itens do instrumento.

A análise de frequência das respostas nas categorias dos itens permitiu encontrar um item que teve um único tipo de resposta: “Csc_02_3 - *As informações da sua organização necessitam de segurança?*”. Esse item apresentou só uma categoria de resposta, ou seja, todos os respondentes afirmaram que a informação necessita de proteção (opção 1). Com base nesta constatação, o item foi retirado da pesquisa por não agregar informação para a construção da escala.

No entanto, o fato do item ter tido só um tipo de resposta levanta as seguintes hipóteses. Esse comportamento pode ter sido causado pelo tamanho ou característica da amostra, ou seja, todos os respondentes da população selecionada têm conhecimento necessário para assinalar corretamente o item. Em sendo esse o caso, deve-se manter o item nas próximas aplicações para verificar se, com o aumento de respondentes, encontra-se alguém que não possua conhecimento suficiente para escolher outra categoria, dado que, nesse caso, os respondentes optaram pela categoria mais elevada do item.

A outra hipótese seria considerar que o item apresenta um problema na sua formulação que induz os respondentes a assinallarem a mesma categoria. Neste caso, o item deverá ser reformulado e reapresentado nas próximas edições.

Independente das hipóteses suscitadas, sugere-se que o item seja mantido nas futuras aplicações com vistas a confirmar ou rejeitar a primeira hipótese, para que, só então, seja tomada a decisão a respeito do item.

A análise revelou, também, a existência de itens cujas categorias apresentavam frequências relativamente baixas. Os itens que apresentaram problema de frequência em suas categorias

foram identificados a fim de se verificar, nas etapas de calibração e análise fatorial, se eles necessitam ter suas categorias recodificadas ou se serão descartados.

4.2.3 Agrupamento das categorias dos itens

Alguns itens que são dicotômicos por definição foram elaborados com quatro categorias de respostas (Nunca, Raramente, Frequentemente e Sempre) com o objetivo de deixar o respondente mais a vontade para expressar a sua opinião, respondendo 'Raramente' a 'Nunca' ou 'Frequentemente' a 'Sempre'. Nesses casos, as categorias foram agrupadas para a configuração dicotômica 'Nunca' (agrupando 'Nunca' e 'Raramente') ou 'Sempre' (agrupando 'Frequentemente' e 'Sempre').

Outra situação que demandou agrupar as categorias dos itens foi identificada durante o processo de avaliação da qualidade do item (tópico 4.2.6 - calibração). Observou-se que as categorias 'Raramente' e 'Frequentemente' não tinham informações suficientes. Desta forma, as categorias 'Raramente' e 'Frequentemente' foram agrupadas e passaram a se chamar 'Às vezes'. Por esse motivo, os itens passaram a ter três categorias ('Nunca', 'Às vezes' e 'Sempre').

Ao tomar essa decisão, verificou-se, no processo de calibração, que o agrupamento das categorias melhorou a qualidade dos itens e que os erros padrões reduziram.

Esse processo de agrupamento das categorias dos itens permitiu, também, a uniformização do instrumento que passou a conter itens com duas ou três categorias.

O resultado final do procedimento de agrupamento pode ser visto no quadro 6 constante do apêndice B e também na figura 8 no apêndice C.

4.2.4 Dimensionalidade do Instrumento

Uma vez que o arquivo estava em condição de ser processado, deu-se início ao procedimento de avaliação da dimensionalidade do instrumento, pela análise fatorial de informação completa, *full-information*.

O critério utilizado para identificar a pertinência do item com um fator foi sugerido por Hair, Black *et al.* (2009). Dado que a amostra tem tamanho $n = 1117$ (ou seja, > 350), a carga fatorial

do item para pertencer ao fator deve ser $\geq 0,30$ e sua comunalidade $\geq 0,20$.

Ao final de quatro execuções do procedimento da análise fatorial, pôde-se identificar um fator (uma dimensão) predominante, que contém um total de 55 itens e contempla as 9 facetas. Essa dimensão (fator) possui uma variância explicada de 38,9%, o que justifica a utilização do modelo unidimensional e a construção da escala de medida.

A tabela 7 apresenta o resultado final da análise fatorial de informação completa.

Tabela 6 - Resultado final da análise fatorial de informação completa.

N	Item	F1	h2	N	Item	F1	h2
1	Csc_01_1	0,49	0,24	29	Rpt_03_3	0,46	0,21
2	Csc_01_2	0,61	0,37	30	Rsc_01_1	0,55	0,30
3	Csc_03_6	0,67	0,45	31	Rsc_01_3	0,67	0,45
4	Csc_03_7	0,70	0,49	32	Rsc_04_2	0,53	0,28
5	Csc_04_1	0,64	0,41	33	Rsc_04_3	0,48	0,23
6	Csc_04_2	0,47	0,22	34	Rsc_06_3	0,66	0,43
7	Csc_05_2	0,57	0,32	35	Rsc_11_3	0,47	0,22
8	Csc_05_3	0,65	0,42	36	Rsc_12_1	0,67	0,45
9	Csc_05_4	0,54	0,29	37	Rsc_12_2	0,73	0,53
10	Csc_06_1	0,44	0,20	38	Rsc_12_6	0,51	0,26
11	Dmc_02_2	0,52	0,27	39	Rsc_13_1	0,47	0,22
12	Etc_01_1	0,69	0,48	40	Rsc_13_2	0,64	0,41
13	Etc_06_1	0,71	0,51	41	Rsc_14_1	0,52	0,27
14	Etc_06_2	0,76	0,57	42	Rsc_14_2	0,64	0,41
15	Etc_06_3	0,69	0,48	43	Rsc_14_3	0,57	0,32
16	Etc_06_4	0,67	0,45	44	Rsc_15_2	0,50	0,25
17	Gts_01_1	0,74	0,55	45	Rsc_16_1	0,57	0,33
18	Gts_01_2	0,71	0,51	46	Rsc_16_2	0,46	0,21
19	Gts_01_3	0,63	0,40	47	Rsc_16_3	0,58	0,34
20	Gts_01_4	0,63	0,40	48	Rsc_16_4	0,65	0,42
21	Gts_01_5	0,79	0,62	49	Rsp_02_1	0,49	0,24
22	Gts_01_6	0,56	0,32	50	Rsp_02_2	0,59	0,35
23	Prj_01_1	0,49	0,24	51	Rsp_02_3	0,65	0,43
24	Prj_02_1	0,72	0,52	52	Rsp_03_1	0,60	0,36
25	Prj_02_2	0,90	0,81	53	Rvl_01_1	0,80	0,64
26	Prj_02_3	0,86	0,74	54	Rvl_01_2	0,66	0,43
27	Rpt_01_2	0,62	0,38	55	Rvl_02_1	0,71	0,51
28	Rpt_01_3	0,54	0,29				

Fonte: Próprio autor

Os itens não pertencentes ao fator dominante, ou seja, aqueles que não atenderam aos requisitos já descritos foram retirados e, portanto, não fazem parte da escala. Contudo, esses itens trazem consigo uma quantidade grande de informações que podem ser úteis para os gestores das organizações. Vale citar, como exemplo, os itens da faceta 'Democracia', agrupamento 01: "*O líder de uma equipe ou organização deve ser capaz de comandar pessoas, atrair seguidores, influenciar e motivar positivamente o comportamento do grupo*" que revelam que 27 % dos respondentes não consideram o chefe um líder e 38% declararam que o chefe não incentiva comportamento favorável à segurança da informação e também não transmite segurança.

4.2.5 Calibração dos itens

Conforme relatado no capítulo 3 - Método, o processo de calibração dos itens foi realizado por meio da função *mirt()* do pacote *MIRT* no ambiente R.

Os resultados do processamento estão apresentados na tabela 8.

Tabela 7 - Estimativas dos parâmetros dos itens na escala (0,1)

Item	a	EP(a)	b1	EP(b1)	b2	EP(b2)
Csc_01_1	0,911	0,200	-1,209	0,275	2,528	0,506
Csc_01_2	1,208	0,237	-0,549	0,157	2,824	0,483
Csc_03_6	1,211	0,339	-2,493	0,511		
Csc_03_7	1,309	0,322	-2,330	0,400		
Csc_04_1	1,199	0,290	-2,424	0,422		
Csc_04_2	0,867	0,192	-1,122	0,270		
Csc_05_2	1,077	0,209	0,420	0,158		
Csc_05_3	1,279	0,245	-0,037	0,131		
Csc_05_4	0,991	0,207	-0,615	0,189		
Csc_06_1	0,815	0,184	0,573	0,213		
Rsp_02_1	0,925	0,209	-3,855	0,797	-0,029	0,169
Rsp_02_2	1,165	0,218	-1,365	0,234	0,288	0,156
Rsp_02_3	1,343	0,209	-1,260	0,185	1,303	0,209

Item	a	EP(a)	b1	EP(b1)	b2	EP(b2)
Rsp_03_1	1,199	0,218	-0,109	0,139		
Rpt_01_2	1,204	0,190	-1,762	0,260	2,124	0,299
Rpt_01_3	1,004	0,190	-1,677	0,303	2,428	0,426
Rpt_03_3	0,856	0,159	-2,560	0,467	0,327	0,178
Etc_01_1	1,423	0,262	-3,152	0,487	1,710	0,251
Etc_06_1	1,548	0,235	-0,762	0,145	1,813	0,233
Etc_06_2	1,764	0,266	-0,579	0,124	1,400	0,173
Etc_06_3	1,464	0,270	-0,444	0,133	1,899	0,276
Etc_06_4	1,400	0,246	-1,536	0,220	1,769	0,274
Gts_01_1	1,662	0,265	-1,411	0,175	1,546	0,209
Gts_01_2	1,579	0,246	-1,719	0,224	1,090	0,160
Gts_01_3	1,341	0,226	-2,110	0,319	0,380	0,131
Gts_01_4	1,291	0,210	-3,061	0,445	0,506	0,137
Gts_01_5	1,909	0,274	-1,683	0,189	1,365	0,162
Gts_01_6	1,056	0,208	-2,866	0,509	1,328	0,266
Dmc_02_2	0,974	0,186	-3,738	0,701	0,872	0,196
Rsc_01_1	1,038	0,177	-0,683	0,179	2,801	0,440
Rsc_01_3	1,381	0,224	-0,386	0,136	2,671	0,370
Rsc_04_2	1,018	0,178	-0,241	0,158	1,860	0,309
Rsc_04_3	0,888	0,184	-4,015	0,791	-1,055	0,246
Rsc_06_3	1,364	0,212	-0,726	0,147	1,151	0,193
Rsc_11_3	0,873	0,169	-4,103	0,767	0,219	0,172
Rsc_12_1	1,350	0,247	-1,867	0,278	2,871	0,448
Rsc_12_2	1,583	0,271	0,697	0,140	2,656	0,369
Rsc_12_6	0,939	0,178	-1,942	0,334	2,203	0,408
Rsc_13_1	0,873	0,165	-2,897	0,526	1,389	0,275
Rsc_13_2	1,325	0,199	-1,736	0,242	1,416	0,204
Rsc_14_1	0,961	0,186	-2,579	0,463	1,062	0,237
Rsc_14_2	1,298	0,209	-0,361	0,141	1,734	0,254

Item	a	EP(a)	b1	EP(b1)	b2	EP(b2)
Rsc_14_3	1,117	0,193	-1,411	0,240	1,803	0,282
Rsc_15_2	0,930	0,206	-2,649	0,530	0,482	0,219
Rsc_16_1	1,089	0,220	-2,870	0,505	-0,802	0,190
Rsc_16_2	0,846	0,186	-3,002	0,638	0,233	0,195
Rsc_16_3	1,151	0,222	0,097	0,159	1,791	0,307
Rsc_16_4	1,335	0,219	-0,666	0,171	0,873	0,169
Prj_01_1	0,898	0,190	0,062	0,175		
Prj_02_1	1,520	0,242	-0,364	0,126	1,221	0,174
Prj_02_2	2,663	0,449	-1,224	0,147	1,087	0,117
Prj_02_3	2,309	0,343	-1,503	0,166	1,111	0,128
Rvl_01_1	1,925	0,299	-0,678	0,129	2,212	0,254
Rvl_01_2	1,287	0,247	0,875	0,176	2,854	0,475
Rvl_02_1	1,520	0,253	-1,561	0,216	2,280	0,300

Fonte: Próprio autor.

A tabela 9 mostra a distribuição dos itens por níveis de qualidade do parâmetro ‘a’, segundo os critérios adotados por Baker (2001) e Rabelo (2013).

Tabela 8 - Frequência dos Itens por Níveis de Qualidade

Nível	Faixa do parâmetro ‘a’	Frequência absoluta	Frequência relativa
Moderado	0,64 A 1,34	36	65,45%
Alto	1,35 A 1,7	14	25,45%
Muito alto	> 1,7	05	9,09%
Total		55	

Fonte: Próprio autor.

A qualidade dos itens também pode ser verificada por meio da Curva Característica do Item – CCI na figura 8 do apêndice C.

Pelo critério adotado e sabendo que todos os itens têm parâmetro de discriminação > 0,8, nenhum item foi retirado do instrumento.

O outro critério utilizado na qualificação do item é a análise do erro padrão das estimativas dos parâmetros ‘a’ e ‘b’. Este

critério leva em consideração a magnitude do erro padrão do item em relação aos erros dos demais itens do instrumento. Também, por este critério, não houve retirada de itens, pois não apresentaram erro padrão em dissonância com os demais itens.

Ao final do processo de calibração o instrumento apresentou a seguinte distribuição de itens por faceta.

Tabela 9 - Frequência por faceta

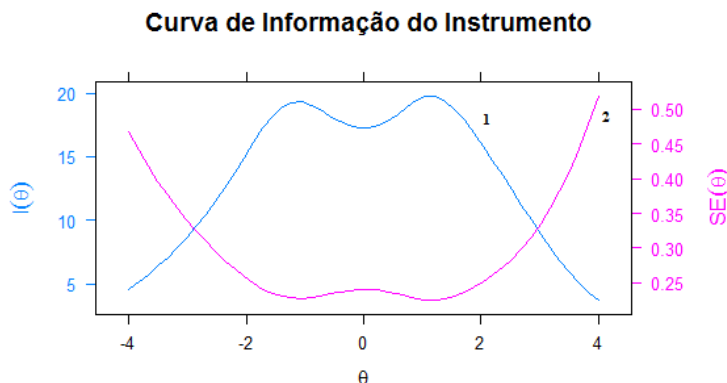
FACETA	FREQUÊNCIA
Análise de Risco	19
Consciência	10
Democracia	1
Ética	5
Gestão de Segurança	6
Projeto de S.I.	4
Reavaliação	3
Responsabilidade	4
Resposta	3
Total	55

Fonte: Próprio autor.

Após todos os testes ficou confirmado que o instrumento de avaliação da cultura organizacional de segurança da informação é constituído de 55 itens.

Pode-se concluir que o instrumento resultante da calibração dos itens tem maior nível de informação entre os tetras θ de -2 e 2 (linha 1). Nesse intervalo, o instrumento é mais preciso (linha 2). Observa-se, também, que acima da média o instrumento está ligeiramente mais informativo, como mostra a figura 6.

Figura 6 - Curva de Informação do Instrumento



Fonte: Próprio autor.

4.3 VALIDAÇÃO DO MODELO

Segundo Brown (2015, p. 74) os critérios que determinam a boa qualidade ou bom ajuste do modelo devem atender no mínimo a estatística $RMSEA < 0,05$ e as estatísticas CIF e $TLI > 0.90$ (índice *goodness-of-fit*). A tabela 11, abaixo, apresenta os resultados obtidos com a aplicação do teste de qualidade do modelo (função M2 do pacote *MIRT*).

Tabela 10 - Parâmetros do teste

Índices	
RMSEA	0,006
RMSEA_5	0,0001
RMSEA_95	0,01
SRMSR	0,03
TLI	0,999
CFI	0,999

Fonte: Próprio autor.

Segundo os resultados obtidos, o modelo gradual unidimensional de Samejima resultante do processo de calibração dos itens apresenta indicativos de validade e garante que o instrumento está bem ajustado.

4.4 VALIDAÇÃO DE CRITÉRIO

Para o teste, os escores dos respondentes foram categorizados para torná-los qualitativos. Em seguida, foi feita uma correlação entre os resultados do item autoavaliação e o escore. O resultado foi uma correlação de 0,99.

Objetivando verificar se os resultados (autoavaliação e escores) não são uma coincidência, foi utilizado o método *crostab* com teste χ^2 qui-quadrado.

A hipótese H_0 do teste χ^2 é: *os resultados obtidos não apresentam relação com os fornecidos na autoavaliação.*

O procedimento de cálculo do teste *qui-quadrado* obteve os seguintes resultados:

$$\chi^2 = 322,1$$

$$gl = 39 \text{ e}$$

$$p \approx 0,000$$

Esses resultados comprovam a rejeição da hipótese H_0 (*os resultados obtidos não apresentam relação com os fornecidos na autoavaliação*), confirmando, portanto, que os resultados obtidos pelo modelo são coerentes com a autoavaliação dos respondentes.

Após o procedimento anterior, os resultados da pesquisa foram apresentados aos especialistas os quais concluíram pela aprovação da escala resultante do modelo desenvolvido.

Em conclusão, tanto a validação de critério por meio de procedimentos estatísticos, quanto aquela realizada pelos especialistas, comprovaram que o instrumento de avaliação desenvolvido mede, efetivamente, o traço latente - cultura organizacional de segurança da informação.

A tabela 15 no apêndice E apresenta os resultados dos cálculos.

4.5 CONSTRUÇÃO E INTERPRETAÇÃO DA ESCALA

A metodologia descrita no tópico 3.10 para a determinação do posicionamento dos itens (nível no qual a probabilidade do respondente escolher uma determinada categoria deve ser maior ou igual a 0,6) resultou no quadro 7 no apêndice F (Distribuição dos Itens por Nível de Proficiência).

O posicionamento dos itens deu origem à escala de medida do nível de cultura organizacional de segurança da informação no padrão (100,10).

A escala foi inicialmente constituída de 13 níveis. Após uma avaliação pelos juízes (especialistas), ficou decidido que a escala seria melhor interpretada se os 13 níveis fossem agrupados e em 5 níveis, de 0 a 4. Os critérios utilizados para o agrupamento dos níveis foram: a complexidade do item; a predisposição ao risco e a relação entre comportamento humano e uso da tecnologia da informação.

A seguir, apresenta-se a interpretação da escala com a definição dos níveis e a análise das organizações e de seus colaboradores, segundo cada faceta pertinente ao nível em que se encontra.

4.5.1 Interpretação da escala

Nível 0 (**Caos**) é o das organizações que não atingiram o nível mínimo (65 pontos) de segurança da informação. As organizações classificadas neste nível estão expostas a todos os tipos de riscos na segurança da informação. Não existe um padrão de comportamento estabelecido e há total desconhecimento sobre o assunto. Todas as iniciativas de segurança nesse nível são isoladas, pessoais, sem fundamento técnico/normativo, ou são puramente intuitivas. Trata-se do nível cujo risco é o mais alto, no qual a organização está mais vulnerável. Pode-se afirmar que não existe uma cultura formalizada sobre segurança da informação e não é possível identificar as facetas.

Nível 1 (**Elementar**) acima de 65 até 75 pontos. Nesse nível, a organização contempla os requisitos mínimos de comportamentos voltados à segurança da informação. Ainda não é observada a relação entre o colaborador e a tecnologia da informação. Tais comportamentos ainda são ocasionais, não frequentes e só às vezes observados. Os seus colaboradores demonstram ter preocupação com a segurança da informação, mas de forma não sistemática e empírica.

- Faceta da Democracia: Os colaboradores devem respeitar os valores, a liberdade de troca de ideias, pensamentos, o livre fluxo de informações, a confidencialidade da informação e da comunicação, a proteção adequada dos dados pessoais, a abertura e a transparência.

- Às vezes os líderes da organização promovem um ambiente participativo com o objetivo de incentivar a equipe na mudança de hábitos.

A liderança é o aspecto mais importante na formação da cultura (SCHEIN, 2004). O fato do líder não dar importância à promoção de um ambiente favorável a mudança de hábitos, torna difícil incutir a cultura de segurança da informação na organização.

- Faceta Consciência: os colaboradores devem entender que as falhas na segurança prejudicam significativamente os sistemas e consequentemente a organização.
- Nesse nível, os incidentes de quebra de sigilo e furto dos dados são considerados pela organização como tendo um impacto severo.

A informação ainda não é considerada pelos colaboradores como sendo um dos patrimônios mais importantes da organização.

- Faceta Ética: preocupa-se com o reconhecimento do respeito ao interesse legítimo de outros participantes e por isso, devem ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação.
- Os colaboradores das organizações nesse nível costumam comentar sobre assuntos internos à organização em locais não apropriados como: no cafezinho, em transportes públicos, elevadores, reuniões e redes sociais, etc.

Tal atitude aumenta o risco de segurança das organizações uma vez que as deixa vulneráveis a ataques do tipo Engenharia Social.

- Faceta Gestão da Segurança da Informação: ela deve ser dinâmica e global.
- Às vezes, as organizações executam as modificações necessárias para adequar às novas necessidades.

O fato da organização não fazer as modificações de forma continuada a coloca em risco, pois fica vulnerável a incidentes causados pela constante evolução e tipos de ataques.

- Às vezes manuseiam os seus dados conforme o planejado.

A gestão da segurança da informação deve ter como premissa executar suas ações segundo uma análise de risco e de acordo com o planejado. O fato do manuseio de dados não ser feito sempre conforme o planejado fragiliza a organização quanto ao princípio da integridade.

- Faceta Avaliação de Risco, todos os participantes devem realizar avaliações de risco em suas atividades. Para Martins e Eloff (2002), todos precisam perceber o risco e assumir a análise do risco como uma atividade cotidiana do trabalho.
- Às vezes, os colaboradores das organizações utilizam em sua senha de acesso números, letras e caracteres especiais.

O fato dos colaboradores não terem o hábito de sempre fazer uso de variedade de caracteres na sua senha de acesso, cria uma vulnerabilidade que aumenta o risco de acesso aos sistemas por pessoas não autorizadas. Quanto maior o número de tipos de caracteres utilizados na composição da senha, mais difícil para ataques do tipo força bruta ou dicionário.

- Às vezes, os colaboradores verificam se o sítio é seguro;
- Às vezes, quando recebem e-mail com anexo, verificam a sua procedência, antes de abrir o anexo.

Tais atitudes deixam a organização vulnerável a ataques do tipo *Phishing*, *Ransomware* (Sequestro de dados), *Trojan* (Cavalo de Troia), todos os tipos de ataques que necessitam de acesso aos sistemas e dispositivos da organização.

- Às vezes, durante o processo de descarte de mídias, os colaboradores verificam o conteúdo da mídia antes do seu descarte;
- Às vezes, simplesmente destrói a mídia.

O risco que a organização incorre é o de não ter o controle do que, quando e como a mídia e quais informações foram descartadas. Isso pode levar a vazamento ou divulgação indevida da informação.

Nível 2 (**Em evolução**) acima de 75 até 90 pontos. Esse nível é chamado de Em Evolução, pois se trata de organizações cujos colaboradores apresentam conhecimentos iniciais, superficiais, sobre o tema segurança da informação e também sobre

tecnologia da informação. Nesse nível as organizações ainda não têm uma cultura organizacional de segurança da informação consolidada, mas dão indícios de estarem se preparando para atingir a consolidação.

As organizações que estão no nível 2 apresentam as características do nível anterior acrescidas das desse nível.

- Faceta Consciência: Os colaboradores devem ter conhecimento da configuração do seu equipamento.
- Os colaboradores dessas organizações já passam a saber qual é o sistema operacional do seu equipamento.

Saber as características da sua ferramenta de trabalho demonstra interesse do colaborador sobre o seu ambiente de trabalho, evitando assim, incidentes de indisponibilidade do equipamento por incompatibilidade com o sistema operacional.

- Faceta Ética: A organização deve ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação.
- Às vezes, nesse nível, os colaboradores, alertam os seus colegas sobre a necessidade de proteger os documentos de trabalho de acesso não autorizado.

Pelo fato da atitude ser realizada às vezes, cria-se uma vulnerabilidade dos dados que, por sua vez, propicia a divulgação não autorizada, infringindo o princípio da confidencialidade.

- Faceta Gestão de Segurança: deve ser dinâmica e global.
- Às vezes, durante o processo de manuseio dos seus dados, levam-se em consideração as diretrizes estabelecidas pela organização, no planejamento, na avaliação do risco de danos ou incidentes de segurança da informação.
- Às vezes, avaliam se os procedimentos estão atendendo às necessidades de segurança da informação.

Em uma gestão de segurança da informação na qual as atitudes frente aos procedimentos estabelecidos pela organização não são realizadas de forma sistemática, a organização se coloca em risco. Este problema pode estar sendo causado pela falta de conhecimento das diretrizes organizacionais de segurança da informação, ou por resistência ao seu cumprimento.

- Faceta Projeto de Segurança e Implementação: Convém que a segurança da informação seja considerada em todas as fases do projeto, independentemente do tipo do projeto.
- Às vezes, nesse nível, as organizações consideram a segurança da informação nas fases de execução e de gerenciamento.
- Às vezes, durante o ciclo de um trabalho ou projeto, que vai desde a concepção até a sua conclusão, os colaboradores da organização reavaliam os procedimentos em busca de falhas ou possíveis incidentes e, formalizam as intercorrências por meio de documento para uso futuro.

Tais atitudes colocam a organização em risco, uma vez que os seus projetos não levam em consideração a segurança da informação e quando encontram algum problema não é documentado, fazendo com que não haja um aprendizado organizacional.

- Faceta Resposta: Os colaboradores da organização devem agir em tempo hábil a fim de prevenir ou impedir possíveis incidentes.
- Às vezes, os colaboradores comunicam à chefia sobre pessoas não identificadas ou estranhas ao local.

O fato do colaborador não informar a ocorrência coloca a organização em risco, pois permite que pessoas alheias ao setor ou à organização possam causar incidentes, como ter acesso a informações privilegiadas, conseguir acesso aos sistemas, furtar documentos e mídias ou, até mesmo, instalar *malwares* nos sistemas de rede.

- Faceta Avaliação de Risco: todos os participantes devem realizar avaliações de risco em suas atividades. Para Martins e Eloff (2002), todos precisam perceber o risco e assumir a análise do risco, como uma atividade cotidiana do trabalho.
- Às vezes, os colaboradores das organizações nesse nível trocam de senha;
- Às vezes, cuidam dos seus equipamentos;
- Às vezes verificam o estado de conservação de equipamentos antes de informar a sua senha.

A troca de senha deve ocorrer com frequência. Esse procedimento diminui a probabilidade de um usuário não autorizado ter acesso a sistemas, contas e redes sem que o verdadeiro proprietário tome ciência. O fato do colaborador cuidar do seu equipamento diminui o risco de indisponibilidade do serviço e também demonstra preocupação e respeito com o local de trabalho. Observar as condições dos equipamentos antes de colocar a senha, demonstra estar atento a possíveis ataques de furto de identificações.

- Às vezes, durante o processo de instalação de um aplicativo, os colaboradores procuram saber sobre sua procedência.

O risco da organização com essa atitude é permitir a espionagem, a indisponibilidade dos sistemas, o sequestro dos seus dados “*Ransomware*” e vazamentos de informações “*wikeleak*”.

- Faceta Responsabilidade: Todos os participantes são responsáveis pela segurança dos sistemas de informação e de redes, eles devem compreender a sua responsabilidade pela segurança desses sistemas e redes.
- Às vezes, os colaboradores da organização comunicam o responsável ou o setor responsável sobre um novo ataque;
- Às vezes checam se o seu equipamento está vulnerável ao ataque.

A postura do colaborador de comunicar, somente às vezes, ao responsável demonstra uma falta de preocupação com a segurança colocando a organização em risco.

- Faceta Reavaliação: As organizações devem analisar e reavaliar a segurança dos sistemas e redes de informação e fazer as modificações necessárias nas políticas, práticas, medidas e procedimentos de segurança.
- Às vezes, os colaboradores reavaliam suas atitudes com respeito à segurança da informação.

Isso coloca a organização em uma situação de vulnerabilidade, pois erros podem estar sendo cometidos e não estão sendo observados.

Nível 3 (**Encaminhado**) acima de 90 até 120 pontos. As organizações posicionadas neste nível começam a demonstrar uma preocupação com a segurança da informação. Embora ainda

exista a condição ‘Às vezes’, os seus colaboradores já estão incutindo o comportamento ‘sempre’ em suas atitudes. Assim, esse nível foi chamado de Encaminhado, pois se percebe que as organizações já apresentam condições que as encaminham em direção a uma cultura de segurança da informação plena.

As organizações que estão nesse nível apresentam as características do nível anterior acrescidas das características inerentes ao nível 3.

- Faceta Consciência: As partes interessadas devem estar cientes da necessidade de garantir a segurança dos sistemas e redes de informação e do que elas podem fazer para melhorar a segurança. Ter conhecimento da configuração e das atualizações disponíveis para seus sistemas.
- Às vezes, os colaboradores verificam o histórico do antivírus e se ele está atualizado;
- Às vezes, sabem qual é a versão do sistema operacional do seu computador, a quantidade de memória RAM, a capacidade de armazenamento do disco e o tipo de conexão do seu computador com a rede.

O risco principal das organizações com essas características é a vulnerabilidade a ataques por *malwares* e, indisponibilidade ou corrupção dos dados devido a insuficiência de processamento. Conhecer as características do equipamento evita o processamento ou armazenamento inadequado dos dados da organização.

- Faceta Democracia: Os colaboradores devem respeitar os valores, a liberdade de troca de ideias, pensamentos, o livre fluxo de informações, a confidencialidade da informação e da comunicação, a proteção adequada dos dados pessoais, a abertura e a transparência.
- Sempre, nas organizações a partir desse nível, os chefes promovem um ambiente participativo para incentivar as mudanças de hábitos de segurança da informação.

O ambiente participativo permite maior eficiência e cumplicidade de todos os colaboradores no processo de estabelecimento de uma cultura em segurança da informação.

- Faceta Ética: Os participantes devem ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação
- Às vezes, os colaboradores alertam os colegas sobre a necessidade de desligar o computador quando não estiver em uso;
- Às vezes, mantem suas mesas limpas / organizadas;
- Às vezes ou sempre, alertam os outros para que bloqueiem o computador quando se afastarem dele.

Os procedimentos éticos da forma como são realizados 'Às vezes' não são eficientes, o que leva a organização a ter dificuldades no acultramento em segurança da informação.

- Faceta Gestão de Segurança: Os participantes devem adotar uma abordagem abrangente para a gestão da segurança.
- Sempre, durante o processo de manuseio dos dados da organização, os colaboradores avaliam os riscos de ocorrência de incidentes como perda, roubo, adulteração e acesso indevido aos dados;
- Sempre levam em consideração a avaliação dos riscos no planejamento do local e da forma como os dados serão armazenados e acessados.
- Sempre levam em consideração as diretrizes estabelecidas pela sua organização no planejamento e executam os processos conforme planejado.
- Sempre avaliam se os procedimentos adotados estão atendendo às necessidades de segurança e, também, executam as modificações necessárias para adequar às novas necessidades de segurança.

A gestão é um dos pilares da governança. Assim sendo, as organizações nesse nível cumprem os requisitos que subsidiam uma boa governança.

- Faceta Projeto de Segurança e Implementação: Convmém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes e que seja considerada, em todas as fases do projeto, independentemente do tipo do projeto.

- As organizações nesse nível já possuem um conjunto de políticas de segurança da informação, embora ainda não completamente implantada;
- Às vezes ou Sempre essas organizações consideram a segurança da informação na fase de definição e de elaboração do projeto;
- Sempre a segurança da informação é considerada nas fases de execução e gerenciamento;
- Sempre, após a conclusão da atividade, projeto ou trabalho, os colaboradores formalizam, por meio de documento, as intercorrências para uso futuro.

Trata-se de uma faceta muito importante no processo de prevenção de incidentes, melhoria contínua da qualidade do serviço e, principalmente, contribuição para o aprendizado organizacional. As atitudes dos colaboradores nesse nível reduzem significativamente o risco de incidentes.

- Faceta Resposta: Os colaboradores da organização devem agir em tempo hábil a fim de prevenir ou impedir possíveis incidentes.
- Sempre os colaboradores da organização comunicam à chefia sobre pessoas não identificadas ou estranhas ao local.

Essa atitude reduz significativamente os riscos que possam causar incidentes de acesso às informações privilegiadas, conseguir acesso aos sistemas, furto de documentos e mídias ou, até mesmo, a instalação *malwares* nos equipamentos.

- Faceta Análise de Risco: todos os participantes devem realizar avaliações de risco em suas atividades. Para Martins e Eloff (2002), todos precisam perceber o risco e assumir a análise do risco, como uma atividade cotidiana do trabalho.
- Às vezes, os colaboradores das organizações, fazem cópia de segurança em mídias externas. (CD, DVD, *Storage*, *Pendrive*,...);
- Às vezes, verificam se as cópias de segurança estão atualizadas;
- Às vezes, ao receber um e-mail com arquivo anexo, os colaboradores passam o antivírus antes de abrir;

- Às vezes ou sempre, ao receber uma mídia (CD, DVD, *Pendrive*,...), passam o antivírus antes de abrir ou executar programas da mídia;
- Sempre verificam a procedência do e-mail antes de abrir o anexo;
- Sempre utilizam números, letras e caracteres especiais misturados em suas senhas;
- Às vezes, os colaboradores criptografam os dados importantes;
- Sempre, ao acessar uma página na Internet, os colaboradores verificam se o sítio é seguro;
- Sempre, antes de utilizar a sua senha, os colaboradores verificam se alguém está observando;
- Às vezes, ao utilizar a sua senha, verificam se estão sendo filmados;
- Sempre, durante o processo de instalação de um aplicativo, os colaboradores verificam a sua procedência;
- Às vezes, ao descartar uma mídia (CD, DVD, disquete, fita magnética, papel, etc.), os colaboradores conferem o seu conteúdo, registra o descarte ou a sua baixa;
- Às vezes ou Sempre, verificam se a mídia está em conformidade com os requisitos para o seu descarte;
- Sempre destrói a mídia.

As atitudes que não são habitualmente sempre executadas pelos colaboradores colocam a organização em risco.

- Faceta Responsabilidade: Todos os participantes são responsáveis pela segurança dos sistemas de informação e de redes.
- Sempre, ao saber de um novo tipo de ataque, os colaboradores alertam os colegas de equipe, comunica o setor responsável e verifica se o seu computador está vulnerável a esse ataque;

Os colaboradores conhecem as suas responsabilidades e atribuições relacionadas à segurança da informação.

- Faceta Reavaliação: Convém que as políticas de segurança da informação sejam analisadas criticamente em intervalos planejados ou quando mudanças signi-

ficativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

- Às vezes, as organizações revisam suas políticas de segurança da informação, bem como convidam os seus colaboradores a participarem da revisão.

O fato das organizações não revisarem, rotineiramente, suas políticas de segurança da informação faz com que estas acabem se tornando ineficientes.

Nível 4 (**Otimizado**) acima de 120. As organizações aqui posicionadas já estão com sua cultura de segurança da informação estabelecida. Nesse nível os colaboradores já entendem que a segurança da informação é uma questão vital para a organização. A preocupação das organizações nesse nível está em encontrar formas e procedimentos mais eficazes e eficientes para atingir uma melhor efetividade.

- Faceta Consciência: Devem estar cientes da necessidade de garantir a segurança dos sistemas e redes de informação e do que elas podem fazer para melhorar a segurança.
- Sempre verificam se o antivírus está atualizado e o seu histórico (Relatório).
- Faceta Ética: Se preocupa com o reconhecimento do respeito ao interesse legítimo de outros participantes e por isso, devem ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação.
- Nunca comentam sobre assuntos internos à organização em locais não apropriados como: no cafezinho, em transportes públicos, elevadores, reuniões e redes sociais, etc;
- Sempre alertam os seus colegas sobre a necessidade de desligar o computador quando não estiver em uso, de manter a mesa limpa/organizada e sempre proteger os documentos de trabalho de acesso não autorizado.
- Faceta Projeto de Segurança e Implementação: Devem integrar a segurança como um elemento essencial dos sistemas e redes de informação

- Sempre, durante o decorrer das atividades, reavaliam os procedimentos em busca de falhas ou de possíveis incidentes;
- Sempre, após a conclusão da atividade projeto ou trabalho, formalizam por meio de documento as intercorrências para uso futuro.
- Faceta Análise de Risco: todos os participantes devem realizar avaliações de risco em suas atividades. Para Martins e Eloff (2002), todos precisam perceber o risco e assumir, como uma atividade cotidiana do trabalho, a análise do risco.
- Sempre fazem cópia de segurança dos seus arquivos profissionais em mídias externas (CD, DVD, *Storage*, *Pendrive*,...);
- Sempre verificam se as cópias de segurança estão atualizadas;
- Sempre verificam a procedência do e-mail antes de abrir o anexo;
- Sempre trocam a sua senha de acesso;
- Sempre criptografa os dados importantes;
- Sempre limpam e higienizam o seu equipamento de trabalho;
- Sempre verificam se está sendo filmado antes de utilizar a sua senha independente da atividade que estão fazendo;
- Sempre verificam se o dispositivo que está utilizando está em bom estado de conservação;
- Sempre, ao descartar uma mídia (CD, DVD, disquete, fita magnética, papel, etc.), registram o descarte ou a baixa da mídia.
- Faceta Reavaliação: Convém que as políticas de segurança da informação sejam analisadas criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
- Sempre revisam as políticas de segurança da informação;
- Sempre convidam os seus colaboradores a participarem da revisão;

- Sempre reavaliam as suas atitudes com respeito à segurança da informação.

Uma organização neste nível apresenta uma baixa probabilidade de vir a sofrer um incidente causado por negligência, omissão ou desconhecimento de seus colaboradores. No entanto, persiste o risco de ocorrer um incidente ocasionado por motivos intencionais.

Conforme a descrição da escala, o nível 3 (Encaminhado) pode ser considerado o nível da estabilidade cultural, uma vez que os seus colaboradores já apresentam ter consciência e atitudes favoráveis à segurança da informação.

Os três níveis anteriores representam um índice de risco elevado, pois cumprem de forma não frequente ‘Às Vezes’ apenas 20% dos pontos de controle.

4.5.2 Posicionamento da organização

Para determinar o posicionamento da organização na escala, o método mais utilizado é o cálculo do escore da organização por meio da média dos escores dos seus colaboradores.

$$escore = \frac{\sum_{i=1}^n escore_i}{n} \quad 15$$

onde:

n = número de respondentes na organização

A tabela 12 mostra o posicionamento das organizações participantes. Como já relatado, a amostra apresenta características (respondentes voluntários) que não garantem a representatividade das organizações participantes desse estudo, razão pela qual não devem ser comparadas entre si.

Tabela 11 - Posicionamento pela Média

Órgão	n	Escore Médio	Desvio Padrão	Escore Mínimo	Escore Máximo	Nível	Nível Mínimo	Nível Máximo
1	20	99,38	11,19	69,45	115,22	3	1	3
2	41	96,31	12,47	67,65	123,83	3	1	4
3	53	97,96	9,40	79,09	122,96	3	1	3
4	320	98,77	9,07	72,14	123,18	3	1	4
5	218	105,71	9,91	72,13	131,89	3	1	4
6	434	98,66	9,59	66,30	127,80	3	1	4
7	31	100,08	7,94	83,13	116,56	3	2	3
Geral	1117	100,00	10,00	66,30	131,89			

Esse método pela média não leva em consideração a distribuição dos colaboradores em cada nível da escala. Supondo, por exemplo, uma organização com 50% dos seus colaboradores no nível 0 e 50% no nível 4, aplicando o critério da média a organização ficaria no nível 2 (Em evolução), o que não expressa a real condição da organização, pois tem muitos colaboradores em situação de baixa proficiência e isso coloca a organização em alto risco de segurança.

Já que o traço latente dessa pesquisa foi definido considerando justamente o elo mais fraco da organização, ou seja, seus colaboradores, é importante propor um segundo método que venha a representar o posicionamento da organização levando em consideração a distribuição dos seus colaboradores nos níveis. Nesse sentido, o posicionamento da organização é decidido em função da concentração dos colaboradores nos cinco níveis.

O quadro 4 apresenta os critérios para uma definição do nível de cultura de segurança da informação na organização, em uma abordagem mais conservadora, pois considera a quantidade de colaboradores nos níveis de alto risco para a segurança da informação da organização.

Quadro 4 - Limites de concentração por nível

Nível	Regra
0 – Caos	A quantidade de colaboradores nesse nível é $\geq 10\%$, independente dos níveis mais elevados.
1 – Elementar	Ter menos de 10 % no nível anterior e a soma dos níveis 0 e 1 $\geq 10\%$
2 – Em Evolução	A totalização dos dois níveis anteriores deve ser menor que 10% e a totalização dos níveis 0, 1 e 2 $\geq 20\%$
3 – Encaminhado	Os níveis 0, 1, 2 devem totalizar menos que 20% e ter mais de 30% no nível 3.
4 – Otimizado	Deve ter mais de 70% dos colaboradores no nível 4

Fonte: Próprio Autor

A tabela 13 representa o posicionamento das organizações participantes conforme as regras do quadro 4.

Tabela 12 - Posicionamento pelo nível de concentração

Organização	Níveis				
	0	1	2	3	4
1	0,00%	5,00%	10,00%	85,00%	0,00%
2	0,00%	7,30%	22,00%	68,30%	2,40%
3	0,00%	0,00%	15,10%	83,00%	1,90%
4	0,00%	0,62%	16,56%	81,56%	1,25%
5	0,00%	0,46%	4,59%	85,32%	9,63%
6	0,00%	1,20%	15,20%	81,80%	1,80%
7	0,00%	0,00%	9,70%	90,30%	0,00%

Fonte: Próprio Autor

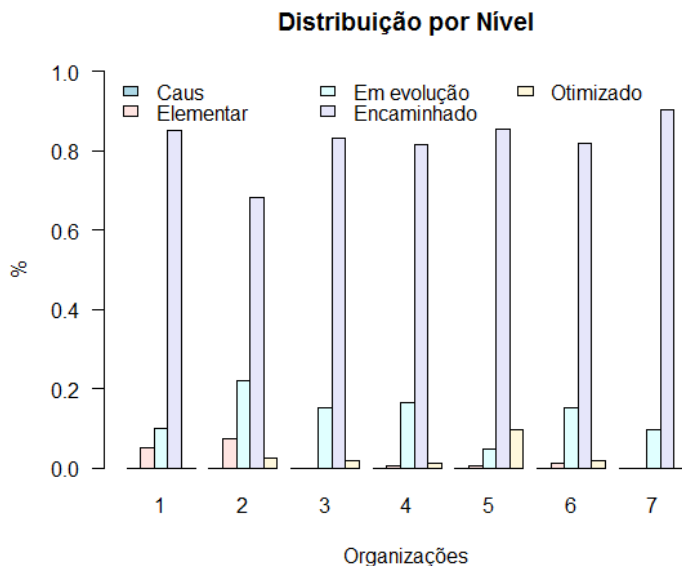
De acordo com a tabela 12 todas as organizações participantes estão classificadas no nível 3 e seus colaboradores variam, em sua maioria, do nível 1 ao 4. As organizações 1, 2, 3, 4 e 6 estão um pouco abaixo da média. A organização 5 está um pouco acima da média e a organização 7 está na média e aparenta ser a mais homogênea.

Já a tabela 13, resultado da aplicação da segunda metodologia, mostra que a organização 2 não está posicionada no nível 3. Isso porque a organização 2 totaliza 29,3% dos colaboradores entre os níveis 0, 1 e 2, satisfazendo a terceira regra.

Os resultados obtidos pelo segundo método estão mais alinhados com a finalidade da pesquisa, uma vez que o foco do estudo é identificar o quão vulnerável a organização está em relação a cultura de segurança da informação.

A figura 7 mostra a distribuição dos escores por nível em cada organização.

Figura 7 - Distribuição dos escores em cada nível nas organizações



Fonte: Próprio autor

4.6 SÍNTESE DO CAPÍTULO

Ao final de quatro execuções chegou-se a um total de 55 itens, que compõe uma única dimensão (fator) e com uma variância explicada de 38,9%.

Os 55 itens foram calibrados resultando em 65 % de itens com parâmetro de discriminação ' α ' moderado, 25% alto e 10 % muito alto.

O modelo foi validado utilizando-se o índice *goodness-of-fit* por meio das estatísticas RMSEA, CIF e TLI. O modelo resultante do processo de calibração satisfaz todos os critérios descritos por Brown (2015p.74).

Na validação de critério, ficou comprovado que o modelo está medindo o traço latente - cultura organizacional de segurança da informação.

Após a análise dos resultados foi construída a escala de cultura de segurança da informação. A escala final ficou dividida em 5 níveis. Nível 0, considerado Caos, no qual as organizações estão sujeitas a todo tipo de incidentes envolvendo segurança da informação. Nível 1, Elementar. Nesse nível as organizações

demonstram alguma preocupação com a segurança da informação e seus colaboradores têm comportamentos básicos, de forma inconstante, de iniciativa pessoal e não normatizada. Nível 2, Em evolução, no qual as organizações começam a apresentar comportamentos sistemáticos e iniciam o desenvolvimento das políticas de segurança da informação. Nível 3, Encaminhado. As organizações nesse nível já possuem sua política de segurança da informação e os colaboradores, em sua maioria, apresentam atitudes seguras e de forma coletiva. Por fim, as organizações no nível 4, Otimizado, já atingiram um nível cultural adequado e passam a aperfeiçoar os seus procedimentos de segurança da informação.

5 CONCLUSÃO E SUGESTÕES PARA TRABALHOS FUTUROS

5.1 CONCLUSÃO

A ampla pesquisa bibliográfica realizada sobre o tema da segurança da informação permitiu a compreensão dos aspectos que influenciam o gerenciamento de segurança da informação nas organizações. Percebeu-se que todo investimento realizado para garantir uma segurança adequada da informação, tanto interna à organização quanto no contexto da integração da cadeia de suprimento, não teria eficácia se não fossem observados o fator humano e sua responsabilidade nesse processo.

Concluiu-se, portanto, que para se avaliar o nível de segurança de informação em uma organização, é necessário avaliar o nível de cultura de segurança da informação.

O propósito desse estudo foi então encontrar um meio pelo qual se pudesse quantificar o nível da cultura organizacional de segurança da informação e construir uma escala interpretada, que permitisse a comparabilidade entre as organizações, em especial aquelas pertencentes a uma cadeia de suprimento, de modo a auxiliar os administradores em suas tomadas de decisão.

Nesse sentido, foi realizada uma revisão da literatura sobre os temas da cultura organizacional, da segurança da informação e da Teoria da Resposta ao item - TRI, alicerces teóricos para o desenvolvimento da pesquisa. Como primeiro resultado e contribuição relevante do estudo, apresentou-se uma proposta de conceito de cultura organizacional aplicada à segurança da informação: *“Trata-se da forma com que o grupo social compartilha, expressa ou manifesta coletivamente os seus conhecimentos, crenças, valores e acordos tácitos sobre segurança da informação, visando, sobretudo, a sobrevivência da organização.”*

Definido o traço latente objeto de avaliação e estabelecidos os seus atributos (facetas), foi possível responder à questão de tese “Como medir o nível da cultura organizacional de segurança da Informação?” com a criação de uma escala de avaliação da proficiência cultural da organização em segurança da informação. A escala foi definida em cinco níveis: 0 – Caos, 1 – Elementar, 2 – Em evolução 3 – Encaminhado e 4 – Otimizado.

Para a construção da escala, foi elaborado um instrumento de avaliação que, após todos os procedimentos de análise e de validação descritos no capítulo 4, resultou em um questionário com 55 itens, abrangendo os nove princípios de cultura organizacional de segurança da informação definidos pela OCDE (2002), denominadas facetas, e os controles de segurança da informação descritos na norma NBR ISO/IEC 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b).

A utilização da TRI, com o modelo de resposta gradual - MRG de Samejima, foi a solução que possibilitou o cálculo dos parâmetros dos itens e, conseqüentemente, a quantificação do traço latente - cultura organizacional de segurança da informação.

O estudo também resultou em produtos elaborados pelo próprio autor, necessários ao atingimento de seu objetivo. São estes: 1) o desenvolvimento de um sistema para captar os dados e controlar a distribuição dos questionários, de forma a garantir que fossem distribuídos igualitariamente entre os respondentes; 2) o desenvolvimento de um aplicativo para crítica visual dos cadernos, visando facilitar e agilizar a análise dos itens do instrumento de coleta.

Diante de tudo que foi exposto, pode-se concluir que o objetivo geral do estudo foi alcançado com a construção de uma escala de medida do nível de cultura de segurança da informação nas organizações, com o utilização da TRI. A contribuição mais importante do estudo decorre, portanto, da construção dessa escala. A utilização da TRI mostrou que a metodologia é capaz de avaliar as características individuais e coletivas considerando a inequidade, que é uma característica inerente à subjetividade. Ou seja, organizações com níveis diferentes de proficiência em cultura de segurança da informação apresentam diferentes escores.

A escala desenvolvida por meio da TRI pode ser aplicada em todos os tipos de organizações, independente do seu tamanho e tipo, e permite a comparação entre as organizações, uma vez que o objeto da TRI é o item. Além disso, a interpretação da escala fornece informações gerenciais relevantes às organizações quanto aos indicadores que efetivamente influenciam na segurança da informação, auxiliando os gestores na tomada de decisões que garantam uma segurança da informação adequada para a sobrevivência da organização na atual sociedade da informação.

5.2 SUGESTÕES PARA TRABALHOS FUTUROS

Tendo em vista a relevância do objeto de estudo e a contribuição dessa pesquisa, para futuros trabalhos, recomenda-se a abordagem dos seguintes tópicos:

1. Fazer um comparativo entre a escala do nível de cultura organizacional de segurança da informação desenvolvida neste estudo com escalas existentes, tais como COBIT, CMMI, ISM3, etc.
2. Estudo da dimensionalidade do instrumento.
3. Inclusão de novos itens no banco de itens.
4. Com a inclusão de mais itens no banco, fazer a implementação de um sistema utilizando Teste Adaptativo (CAT).
5. Validar a escala em outros países (Aculturamento).

REFERÊNCIAS

AJZEN, I. The theory of planned behavior. **Organizational Behavior and Human Decision Processes**, v. 50, n. 2, p. 179-211, 1991/12/01/ 1991. ISSN 0749-5978. Disponível em: < <http://www.sciencedirect.com/science/article/pii/074959789190020T> >.

ALFAWAZ, S.; NELSON, K.; MOHANNAK, K. **Information security culture: a behaviour compliance conceptual framework.** Proceedings of the Eighth Australasian Conference on Information Security - Volume 105. Brisbane, Australia: Australian Computer Society, Inc.: 47-55 p. 2010.

ALNATHEER, M.; NELSON, K. Proposed framework for understanding information security culture and practices in the Saudi context. **Australian Information Security Management Conference**, 2009.

ANDERSON, J. M. Why we need a new definition of information security. **Computers & Security**, v. 22, n. 4, p. 308-313, 2003/05/01/ 2003. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404803004073> >.

ANDRADE, D. F.; TAVARES, H. R.; VALLE, R. C. **Teoria da Resposta ao Item: Conceitos e Aplicações**. São Paulo: ABE - Associação Brasileira de Estatística, 2000.

ARAUJO, E. A. C.; ANDRADE, D. F.; BORTOLOTTI, S. L. V. Teoria de Resposta ao Item. **Rev Esc Enferm USP**, v. 43, p. 1000 - 1007, 2009. Disponível em: < <http://www.scielo.br/pdf/reeusp/v43nspe/a03v43ns.pdf> >. Acesso em: 29/11/2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799. Tecnologia da informação: Técnicas de segurança: Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT 2005.

_____. **NBR ISO/IEC 27005**. Tecnologia da informação: Técnicas de segurança: Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT 2011.

_____. **NBR ISO/IEC 27001**. Tecnologia da informação: Técnicas de segurança: Sistemas de gestão da segurança da informação: Requisitos. Rio de Janeiro: ABNT 2013a.

_____. **NBR ISO/IEC 27002**. Tecnologia da informação: Técnicas de segurança: Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT 2013b.

_____. **NBR ISO/IEC 27032**. Information technology - Security techniques - Guidelines for cybersecurity. ABNT. Rio de Janeiro: ABNT: 62 p. 2015.

ASTAKHOVA, L. V. The concept of the information-security culture. **Scientific and Technical Information Processing**, v. 41, n. 1, p. 22-28, 2014/01/01 2014. ISSN 0147-6882. Disponível em: < <http://dx.doi.org/10.3103/S0147688214010067> >.

BAKER, F. B. **THE BASICS OF ITEM RESPONSE THEORY**. 2. EUA: ERIC Clearinghouse on Assessment and Evaluation, 2001. ISBN 1-886047-03-0. Disponível em: < <http://echo.edres.org:8080/irt/baker/final.pdf> >. Acesso em: 16-fev-2015.

BALI, R. C. G. A. B., C. MISCO: a conceptual model for MIS implementation in SMEs. **Information Research**, v. 4, n. 4, 1999. Disponível em: < <http://informationr.net/ir/4-4/paper61.html> >.

BANDYOPADHYAY, T.; JACOB, V.; RAGHUNATHAN, S. Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. **Information Technology and Management**, v. 11, n. 1, p. 7-23, 2010. ISSN 1573-7667. Disponível em: < <http://dx.doi.org/10.1007/s10799-010-0066-1> >.

BARROS, G. T. F. **PROCEDIMENTOS PARA A CONSTRUÇÃO DE INDICADORES POR MEIO DA TEORIA DE RESPOSTA AO ITEM: A CRIAÇÃO DE UMA MEDIDA DE NÍVEL SOCIOECONÔMICO FAMILIAR**. 2016. 159 (Mestrado). Programa de Pós Graduação em Métodos e Gestão em Avaliação, Universidade Federal de Santa Catarina, Florianópolis.

BEATON, A. E.; ALLEN, N. L. Chapter 6: Interpreting Scales Through Scale Anchoring. **Journal of Educational Statistics**, v. 17, n. 2, p. 191-204, 1992. Disponível em: < <http://journals.sagepub.com/doi/abs/10.3102/10769986017002191> >.

BOCK, R. D.; GIBBONS, R.; MURAKI, E. Full-Information Item Factor Analysis. **Applied Psychological Measurement**, v. 12, n. 3, p. 261-280, 1988/09/01 1988. ISSN 0146-6216. Disponível em: < <https://doi.org/10.1177/014662168801200305> >. Acesso em: 2017/11/04.

BORTOLOTTI, S. V. **Resistência à Mudança Organizacional: Medida de Avaliação Por Meio Da Teoria Da Resposta Ao Item**. 2010. 291 Doutorado (Doutorado). Engenharia de Produção, Universidade Federal de Santa Catarina, Universidade Federal de Santa Catarina.

BRADY, W. TQM and Organizational Culture: A Case Study. **The Quality Management Journal**, v. 11, n. 2, p. 42, 2004. ISSN 1068-6967. Disponível em: < http://link.periodicos.capes.gov.br/sfxlcl41?url_ver=Z39.88-2004&rft_val_fmt=info%3Aofi%2Ffmt%3Akev%3Amtx%3Ajournal&genre=article&sid=ProQ%3AProQ%3A&atitle=TQM%20and%20Organizational%20Culture%3A%20A%20Case%20Study&title=The%20Quality%20Management%20Journal&issn=10686967&date=2004-04-01&volume=11&issue=2&spage=42&au=W%20Brady%20Boggs&isbn=&jtitle=The%20Quality%20Management%20Journal&bttitle=&rft_id=info%3Aeric%2F&rft_id=info%3Adoi%2F >.

BRASIL. **Orientações para elaboração de itens para a Avaliação Nacional de Jovens e Adultos.** Brasília: INEP, 2006.

_____. **Instrução Normativa Nº 1, de 13 de junho de 2008**
- **GSIPR.** REPÚBLICA, G. D. S. I. D. P. D. Brasil: Diário Oficial da União 2008.

BREIER, J.; HUDEC, L. **New approach in information system security evaluation.** Satellite Telecommunications (ESTEL), 2012 IEEE First AESS European Conference on: 1-6 p. 2012.

BROWN, T. A. **Confirmatory Factor Analysis for Applied Research.** New York: THE GUILFORD PRESS, 2015.

CADLE, J.; YEATES, D. **Project Management for Information Systems.** 5ª. london: Prentice Hall, 2008. ISBN 978-0-13-206858-1.

CHALMERS, R. P. mirt: A Multidimensional Item Response Theory Package for the R Environment. **Journal of Statistical Software**, v. 48, n. 6, 2012.

CHANG, S. E.; LIN, C. S. Exploring organizational culture for information security management. **Industrial Management & Data Systems**, v. 107, n. 3, p. 438-458, 2007. Disponível em: <
<http://www.emeraldinsight.com/doi/abs/10.1108/02635570710734316> >.

CHEN, C. C.; MEDLIN, B. D.; SHAW, R. S. A cross-cultural investigation of situational information security awareness programs. **Information Management & Computer Security**, v. 16, n. 4, p. 360-376, 2008. Disponível em: <
<http://www.emeraldinsight.com/doi/abs/10.1108/09685220810908787> >.

CHENG, X.; LI, M.; ZHAO, H. **Information security evaluation of e-government systems.** 2007. 532-535 ISBN

978-7-5352-3854-2. Disponível em: < <Go to ISI>://WOS:000250998700134 >.

CHIA, P. A.; MAYNARD, S. B.; A.B., R. **Exploring Organisational Security Culture: Developing A Comprehensive Research Model.** Proceedings of IS ONE World Conference. Las Vegas, USA. 2002.

COMMITTEE ON NATIONAL SECURITY SYSTEMS, C. **Committee on National Security Systems (CNSS) Glossary.** (IE414), C. S. USA: National Security Agency: 160 p. 2015.

CONNOLLY, L.; LANG, M. Information Systems Security: The Role of Cultural Aspects in Organizational Settings. **AIS Electronic Library (AISEL)**, 2013. Disponível em: < <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1037&context=wisp2012> >.

CORRISS, L. **Information security governance: integrating security into the organizational culture.** Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies. Austin, Texas, USA: ACM: 35-41 p. 2010.

CRUZ, R. M.; ALCHIERI, J. C. **Avaliação psicológica: Conceito, métodos e instrumentos.** São Paulo: Casa do Psicólogo, 2003.

DA VEIGA, A.; ELOFF, J. H. P. An information security governance framework. **Information Systems Management**, v. 24, n. 4, p. 361-372, 2007. Disponível em: < <http://www.scopus.com/inward/record.url?eid=2-s2.0-35148886676&partnerID=40&md5=acfa9b73d82180c78b962934bd397a0b> >.

DA VEIGA, A.; MARTINS, N.; ELOFF, J. H. Information security culture-validation of an assessment instrument. **Southern African Business Review**, v. 11, n. 1, p. 147-166, 2007. ISSN 1561-896X.

DEAL, T. E.; KENNEDY, A. A. **Corporate cultures : the rites and rituals of corporate life.** New York: Addison-Wesley, 1982.

DENISON, D. R.; HAALAND, S.; GOELZER, P. Corporate Culture and Organizational Effectiveness: Is Asia Different From the Rest of the World? **Organizational Dynamics**, v. 33, n. 1, p. 98-109, 2004.

DHILLON, G. Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. **Computers & Security**, v. 20, n. 2, p. 165-172, 4/1/ 2001. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404801002097> >.

DHILLON, G. **Principles of Information Systems Security: Text and Cases**. New York, NY: John Wiley and Sons, 2007. ISBN 978-0471450566.

DHILLON, G.; TEJAY, G.; HONG, W. **Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations** Proceedings of the 40th Hawaii International Conference on System Sciences. Hawaii: IEEE Computer Society 2007.

DIAS, A. et al. **Metodologia para análise de risco: Mitigação de perda de SF6 em disjuntores**. Florianópolis, SC: Nova Letra Gráfica & Editora: 1304 p. 2011.

DOJKOVSKI, S.; LICHTENSTEIN, S.; WARREN, M. Enabling information security culture: influences and challenges for Australian SMEs. Australasian Conference on Information Systems (21st : 2010 : Brisbane, Qld.), 2010. Brisbane, Qld. ACIS, 1-3 Dec. 2010.

ELOFF, M. M.; VON SOLMS, S. H. Information Security Management: An Approach to Combine Process Certification And Product Evaluation. **Computers & Security**, v. 19, n. 8, p. 698-709, 12/1/ 2000. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404800080196> >.

EMBRETSON, S. R., S. **Item response theory for psychologists**. Mahwah, NJ: Lawrence Erlbaum Associates, 2000.

EMILIANO, P. C. et al. **CRITÉRIOS DE INFORMAÇÃO DE AKAIKE VERSUS BAYESIANO: ANÁLISE COMPARATIVA**. 19º SINAPE - Simpósio Nacional de Probabilidade e Estatística. São Pedro-SP: Associação Brasileira de Estatística (ABE). 2010.

FERNANDES, K. R.; ZANELLI, J. C. O processo de construção e reconstrução das identidades dos indivíduos nas organizações. **Revista de Administração Contemporânea**, v. 10, p. 55-72, 2006. ISSN 1415-6555. Disponível em: < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1415-65552006000100004&nrm=iso >.

FURNELL, S. IFIP workshop – Information security culture. **Computers & Security**, v. 26, n. 1, p. 35, 2// 2007. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404806001854> >.

FURNELL, S. M.; JUSOH, A.; KATSABAS, D. The challenges of understanding and using security: A survey of end-users. **Computers & Security**, v. 25, n. 1, p. 27-35, 2// 2006. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404805002038> >.

HAGBERG, R.; HEIFETZ, J. Corporate Culture: Telling the CEO the Baby is Ugly. San Mateo, CA, 1997. Disponível em: < <http://www.hagbergconsulting.com/articles-research.html> >. Acesso em: 25/fev/2015.

HAIR, J. F. et al. **Análise multivariada de dados**. 6ª. Porto Alegre Bookman, 2009. ISBN 978-85-7780-534-1.

HAMBLETON, R. K.; SWAMINATHAN, H.; ROGERS, H. J. **Fundamentals of Item Response Theory**. Newbury Park CA: Sage Publications, 1991. ISBN 978-0803936478.

HOFSTEDE, G. Cultural constraints in management theories. **The Academy of Management Executive**, v. 7, n. 1, p. 81-94, Feb 1993 1993.

HU, Q. et al. Top management championship and individual behaviour towards information security: an integrative model. ECIS 2008 Proceedings, 2008.

_____. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. **Decision Sciences**, v. 43, n. 4, p. 615-660, 2012. ISSN 1540-5915. Disponível em: < <http://dx.doi.org/10.1111/j.1540-5915.2012.00361.x> >.

IT GOVERNANCE INSTITUTE. **Information Security Governance: Guidance for Boards of Directors and Executive**. IT Governance Institute. United States of America. 2006. (1-933284-29-3)

JOHNSON, S. O. et al. Measurement and improvement of information security culture. **MEASUREMENT AND CONTROL-LONDON-INSTITUTE OF MEASUREMENT AND CONTROL**-, v. 39, n. 2, p. 52, 2006. ISSN 0020-2940.

JOHNSON, M. E.; GOETZ, E. Embedding Information Security into the Organization. **Security & Privacy, IEEE**, v. 5, n. 3, p. 16-24, 2007. ISSN 1540-7993.

KARLSSON, F.; ÅSTRÖM, J.; KARLSSON, M. Information security culture – state-of-the-art review between 2000 and 2013. **Information and Computer Security**, v. 23, n. 3, p. 246-285, 2015. Disponível em: < <http://www.emeraldinsight.com/doi/abs/10.1108/ICS-05-2014-0033> >.

KAROKOLA, G. R.; KOWALSKI, S.; YNGSTRÖM, L. **Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View**. Proceedings of the 5th International Symposium on Human

Aspects of Information Security & Assurance: HAISA: 58-73 p. 2011.

KOLEN, M. J.; BRENNAN, R. L. **Test Equating, Scaling, and Linking: Methods and Practices**. Third Edition. New York: Springer, 2014. ISBN 978-1-4939-0316-0.

KRAEMER, S.; CARAYON, P. Computer and information security culture: findings from two studies. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2005. SAGE Publications. p.1483-1488.

LARAIA, R. D. B. **Cultura: um conceito antropológico**. 14^a. Rio de Janeiro: Jorge Zahar 2001. 117 ISBN 85-7110-438-7.

LEIDNER, D. E.; KAYWORTH, T. A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. **Management Information Systems Quarterly**, v. 30, n. 2, p. 357 -399, 2006.

LI CAI; MARKATOS, E. P. Limited-information goodness-of-fit testing of hierarchical item factor models. **British Journal of Mathematical & Statistical Psychology**, v. 66, n. 2, p. 245 -276, 2013.

LIM, J. S. et al. Embedding Information Security Culture Emerging Concerns and Challenges. PACIS, 2010. p.43.

LORD, F. M. **Applications of item response theory to practical testing problems**. Hillsdale NJ: Erlbaum, 1980.

LOWRY, P. et al. Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse. **Journal of Business Ethics**, v. 121, n. 3, p. 385-401, 2014/05/01 2014. ISSN 0167-4544. Disponível em: < <http://dx.doi.org/10.1007/s10551-013-1705-3> >.

LUO, X.; WARKENTIN, M.; JOHNSTON, A. C. The impact of national culture on workplace privacy expectations in the

context of information security assurance. AMCIS 2009 Proceedings, 2009. p.521.

MALCOLMSON, J. What is security culture? Does it differ in content from general organisational culture? , Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on, 2009. 5-8 Oct. 2009. p.361-366.

MARTINS, A.; ELOFF, J. Information Security Culture. In: GHONAIMY, M. A.; EL-HADIDI, M. T., *et al* (Ed.). **Security in the Information Society**: Springer US, v.86, 2002. cap. 16, p.203-214. (IFIP Advances in Information and Communication Technology).

MCCOY, B.; STEPHENS, G.; STEVENS, K. J. An investigation of the impact of corporate culture on employee information systems security behavior. ACIS Proceedings, 2009.

MENEGON, L. S. **Mensuração de Conforto e Desconforto em Poltrona de Aeronave pela Teoria da Resposta ao Item**. 2013. (Doutorado). Engenharia de Produção, Universidade Federal d Santa Catarina, Florianópolis, SC.

MIGUEL, P. A. C. et al. **Metodologia de Pesquisa em Engenharia de Produção e Gestão de Operações**. 2ª. Rio de Janeiro: Elsevier: ABEPRO, 2012. ISBN 9788535248913.

MILLER, W. C. P. Behavior Models. In: SCHOOL, W. (Ed.). **Helping the Obese Patient Find Success**. USA: Western School, 2010. cap. 7,

MITNICK, K. D.; SIMON, W. L. **The art of deception – controlling the human element of security**. Indianapolis: Wiley Publishing, 2002.

NADLER, S. S.; KROS, J. F. AN INTRODUCTION TO SARBANES-OXLEY AND ITS IMPACT ON SUPPLY CHAIN MANAGEMENT. **Journal of Business Logistics**, v. 29, n. 1, p. 241-255, 2008. ISSN 2158-1592. Disponível em: < <http://dx.doi.org/10.1002/j.2158-1592.2008.tb00077.x> >.

NATIONAL CYBER SECURITY TASK FORCE. **INFORMATION SECURITY GOVERNANCE: A CALL TO ACTION**. Department of Homeland Security. EUA. 2004

NGO, L.; ZHOU, W.; WARREN, M. Understanding Transition towards Information Security Culture Change. AISM, 2005. p.67-73.

OCDE. **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. July 2002. 2002

OKERE, I.; VAN NIEKERK, J.; CARROLL, M. Assessing information security culture: A critical analysis of current approaches. Information Security for South Africa (ISSA), 2012, 2012. 15-17 Aug. 2012. p.1-8.

ONU. **UN_resolution_58_199 - Creation of a global culture of cybersecurity and the protection of critical information infrastructures** ONU. N.Y. 2004.

_____. **UN_resolution_64_211 - Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information** ONU. N.Y. 2010.

PARSONS, K. et al. A study of information security awareness in Australian government organisations. **Information Management & Computer Security**, v. 22, n. 4, p. 334-345, 2014. Disponível em: < <http://www.emeraldinsight.com/doi/abs/10.1108/IMCS-10-2013-0078> >.

PARSONS, K. M. et al. The Influence of Organizational Information Security Culture on Information Security Decision Making. **Journal of Cognitive Engineering and Decision Making**, v. 9, n. 2, p. 117-129, 2015. Disponível em: < <http://journals.sagepub.com/doi/abs/10.1177/1555343415575152> >.

PASQUALI, L. **Psicometria: Teoria e Aplicações**. Brasília, : UnB, 1997.

PASQUALI, L. **Psicometria dos testes na psicologia e na educação**. 2. Petrópolis - RJ: Vozes, 2004.

PASQUALI, L. Psicometria Psicometría Psychometrics. **Revista da Escola de Enfermagem da USP**, v. 43, n. spe, p. 992, 2009. ISSN 00806234.

PASQUALI, L.; PRIMI, R. Fundamentos da teoria da resposta ao item: TRI. **Avaliação Psicológica**, v. 2, p. 99-110, 2003. ISSN 1677-0471. Disponível em: < http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-04712003000200002&nrm=iso >.

PONEMON INSTITUTE. **The Human Factor in data Protection WP FINAL**. 2012

_____. **2016 Cost of Data Breach Study: Impact of Business Continuity Management**. Ponemon Institute. Traverse City, EUA. 2016

PONEMON INSTITUTE; IBM SECURITY. **2017 Cost of Data Breach Study: Global Overview**. Ponemon Institute LLC. Traverse CityI, EUA: 06-2017. 2017

PRESSMAN, R. S. **Engenharia de Software**. 3ª. São Paulo: Makron Books do Brasil Editora Ltda, 1995.

PWC. **Pesquisa Global de Segurança da Informação 2014 - PwC**. São Paulo. 2014

QUINN, R. E.; SPREITZER, G. M. **The Psychometrics of the Competing Values Culture Instrument and an Analysis of the Impact of Organizational Culture on Quality of Life**. Emerald, 1991. Disponível em: < <https://books.google.com.br/books?id=tiHJlGEACAAJ> >.

RABELO, M. L. **Avaliação Educacional: fundamentos, metodologia e aplicações no contexto brasileiro**. Rio de Janeiro: SBM - Sociedade Brasileira de Matemática, 2013.

RAISCH, D. Anos 90 e o Downsizing. 2014. Disponível em: < <http://ibmmainframe50anos.blogspot.com.br/2014/01/anos-90-e-o-downsizing.html> >. Acesso em: 01-08-2017.

RASHID, R. M.; ZAKARIA, O.; ZULHEMAY, M. N. THE RELATIONSHIP OF INFORMATION SECURITY KNOWLEDGE (ISK) AND HUMAN FACTORS: CHALLENGES AND SOLUTION. **Journal of Theoretical and Applied Information Technology**, v. 57, n. 1, 2013.

RUIGHAVER, A. B.; MAYNARD, S. B.; WARREN, M. Ethical decision making: Improving the quality of acceptable use policies. **Computers & Security**, v. 29, n. 7, p. 731-736, 10// 2010. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404810000386> >.

SAMEJIMA, F. Estimation of latent ability using a response pattern of graded scores. **Psychometrika**, v. 17, 1969. Disponível em: < <https://www.psychometricsociety.org/sites/default/files/pdf/MN17.pdf> >.

SCHEIN, E. H. **Organizational Culture and Leadership**. 3º. Jossey-Bass, 2004. ISBN 0-7879-6845-5.

_____. **The Corporate Culture Survival Guide**. San Francisco, CA: Jossey-Bass, 2009. ISBN 978-0-470-29371-3.

SCHLIENGER, T.; TEUFEL, S. Analyzing information security culture: increased trust by an appropriate information security culture. 14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings., 2003. 1-5 Sept. 2003. p.405-409.

SILVA, E. L. D.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4ª. Florianópolis: UFSC, 2005.

SINDHUJA, P. Impact of information security initiatives on supply chain performance: An empirical investigation. **Information Management & Computer Security**, v. 22, n. 5, p. 450-473, 2014. Disponível em: < <http://www.emeraldinsight.com/doi/abs/10.1108/IMCS-05-2013-0035> >.

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

<http://www.emeraldinsight.com/doi/abs/10.1108/09685220010371394> >.

STAMBUL, M. A.; RAZALI, R. An assessment model of information security implementation levels. Electrical Engineering and Informatics (ICEEI), 2011 International Conference on, 2011. 17-19 July 2011. p.1-6.

SYMANTEC. Pesquisa da Symantec Revela que Informações Digitais Custam US\$ 1,1 trilhão de Dólares às Empresas. 2012. Disponível em: <

http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20120717_01 >. Acesso em: 09/12/2013.

TEZZA, R. **Modelagem Multidimensional para Mensurar Qualidade em Website de E-Commerce Utilizando a Teoria da Resposta ao Item**. 2012. 182 (Doutorado). Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis - SC.

THOMSON, K.-L.; VON SOLMS, R. Information security obedience: a definition. **Computers & Security**, v. 24, n. 1, p. 69-75, 2// 2005. ISSN 0167-4048. Disponível em: <
<http://www.sciencedirect.com/science/article/pii/S0167404804002627> >.

_____. Towards an Information Security Competence Maturity Model. **Computer Fraud & Security**, v. 2006, n. 5, p. 11-15, 5// 2006. ISSN 1361-3723. Disponível em: <
<http://www.sciencedirect.com/science/article/pii/S1361372306703566> >.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação**. 2ª. Brasília: 2007. Disponível em: < www.tcu.gov.br >.

TROMPETER, C. M.; ELOFF, J. H. P. A Framework for the Implementation of Socio-ethical Controls in Information Security. **Computers & Security**, v. 20, n. 5, p. 384-391, 7/1/ 2001. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404801005077> >.

VAN NIEKERK, J. F.; VON SOLMS, R. Information security culture: A management perspective. **Computers & Security**, v. 29, n. 4, p. 476-486, 6// 2010. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404809001126> >.

VARGAS, V. D. C. C. D. **Medida padronizada para avaliação de intangíveis organizacionais por meio da teoria da resposta ao item**. 2007. 207 (Doutorado). Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, SC.

VON SOLMS, B. Information Security — The Third Wave? **Computers & Security**, v. 19, n. 7, p. 615-620, 11/1/ 2000. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404800070218> >.

_____. Information Security governance: COBIT or ISO 17799 or both? **Computers & Security**, v. 24, n. 2, p. 99-104, 3// 2005. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S0167404805000210> >.

_____. Information Security – The Fourth Wave. **Computers & Security**, v. 25, n. 3, p. 165-168, 5// 2006. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S016740480600054X> >.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers and Security**, v. 38, p. 97-102, 2013. ISSN 01674048 (ISSN). Disponível em: <

<http://www.scopus.com/inward/record.url?eid=2-s2.0-84885188079&partnerID=40&md5=690f82349dba89b461b06078ddf3600d>

http://ac.els-cdn.com/S0167404813000801/1-s2.0-S0167404813000801-main.pdf?_tid=21fcf8ec-0d22-11e4-b001-00000aab0f02&acdnat=1405540277_081f7deeb805171042682b6e167e03ea >.

VON SOLMS, R.; VON SOLMS, B. From policies to culture. **Computers and Security**, v. 23, n. 4, p. 275-279, 2004. Disponível em: <

<http://www.scopus.com/inward/record.url?eid=2-s2.0-2942564710&partnerID=40&md5=8141283f17eeda52e0442e1aff148b4f> >.

VROOM, C.; VON SOLMS, R. Towards information security behavioural compliance. **Computers & Security**, v. 23, n. 3, p. 191-198, 5// 2004. ISSN 0167-4048. Disponível em: < <http://www.sciencedirect.com/science/article/pii/S016740480400032X> >.

APÊNDICE A – Itens por Diretriz

Quadro 5 - Itens por Diretriz

Diretriz	Consciência					
Definição	As partes interessadas devem estar cientes da necessidade de garantir a segurança dos sistemas de informação e de redes, e do que elas podem fazer para melhorar a segurança.					
Descrição	- Os participantes devem entender que as falhas na segurança podem prejudicar significativamente os sistemas e redes sob seu controle, bem como os dos outros. - Os participantes devem, também, ter conhecimento da configuração e das atualizações disponíveis para seus sistemas, do lugar que ocupam nas redes e das boas práticas que possam implementar para melhorar a segurança. - Os participantes devem considerar as necessidades dos outros participantes.					
Id_Item	Item	Categorias				
Csc_01_0	Os "malwares" são programas que causam danos aos sistemas computadorizados, como destruição e/ou roubo de dados.	Nunca	Raramente	Frequentemente	Sempre	N. A.
Csc_01_1	Com que frequência você verifica se o antivírus está atualizado?	0	1	2	3	9
Csc_01_2	Com que frequência você verifica o histórico (Relatório) do antivírus?	0	1	2	3	9

Id_Item	Item	Categorias	
Csc_02_0	O patrimônio de uma organização é o conjunto de seus bens e direitos. Em sua opinião:	Não	Sim
Csc_02_1	As informações da organização têm valor financeiro?	0	1
Csc_02_2	As informações integram o patrimônio da organização	0	1
Csc_02_3	As informações da sua organização necessitam de segurança?	0	1

Id_Item	Item	Categorias		
Csc_03_0	Em sua opinião, qual seria o impacto na sua organização caso ocorressem os incidentes a seguir?	Nenhum	Leve ¹	Severa ²
Csc_03_1	A perda dos dados e informações.	0	1	2
Csc_03_2	Acesso indevido aos dados e informações.	0	1	2
Csc_03_3	Adulteração dos dados.	0	1	2
Csc_03_4	Divulgação não autorizada das informações	0	1	2
Csc_03_5	Interrupção ou indisponibilidade dos serviços (Internet, Acessos remotos, Banco de dados, etc)	0	1	2
Csc_03_6	Quebra do sigilo da informação.	0	1	2
Csc_03_7	Furto dos dados e informações.	0	1	2

¹Não afeta a credibilidade²Afeta a credibilidade

Id_Item	Item	Categorias		
Csc_04_0	Sobre o sistema operacional do seu computador, você:	Não	Sim	N.A.
Csc_04_1	Sabe qual é o sistema operacional do seu equipamento?	0	1	9
Csc_04_2	Sabe qual a versão do sistema operacional do seu computador?	0	1	9
Csc_04_3	Sabe se o seu sistema operacional está atualizado?	0	1	9
Csc_05_0	Sobre o equipamento que utiliza, você:	Não	Sim	N.A.
Csc_05_1	Sabe qual é o tipo de processador (Marca, modelo, etc) ?	0	1	9
Csc_05_2	Sabe qual é a quantidade de memória RAM?	0	1	9
Csc_05_3	Sabe qual a capacidade de armazenamento do disco?	0	1	9
Csc_05_4	Sabe o tipo de conexão do seu computador com a rede?	0	1	9

Id_Item	Item	Categorias		
Csc_06_0	A classificação da informação é uma etapa muito importante para a segurança da informação. Sobre a classificação da informação na sua organização.	Não sei informar	Não Implementado	Sim Implementado
Csc_06_1	Você sabe se sua organização tem os procedimentos e diretrizes para classificação da informação implementados?	0	1	2

Diretriz	Responsabilidade		
Definição	Todos os participantes são responsáveis pela segurança dos sistemas de informação e de redes		
Descrição	- Eles devem compreender a sua responsabilidade pela segurança desses sistemas e redes. - Devem prestar contas, na razão de suas funções individuais. - Os participantes devem, regularmente, rever e avaliar suas próprias políticas, práticas, medidas e procedimentos para se assegurarem que estão adequados ao seu ambiente. - Os participantes devem considerar a segurança dos sistemas e redes e divulgar as informações adequadas, incluindo atualizações em tempo hábil		
Id_Item	Item	Gabarito	Categorias
Rsp_01_0	Em sua opinião, quem é o responsável por garantir a segurança da informação na sua organização?		
Rsp_01_1	Ninguém.	0	0
	A sua chefia.	0	1
	O setor de segurança da informação	0	2
	Os colaboradores da organização.	1	5
	Os colaboradores que trabalham na manutenção dos dados e informações da organização.	0	3
	Os técnicos de rede.	0	4

Id_Item	Item	Categorias			
Rsp_02_0	Você soube de um novo tipo de ataque a computadores. Você:	Nunca	Raramente	Frequentemente	Sempre
Rsp_02_1	Alerta os colegas de equipe	0	1	2	3
Rsp_02_2	Comunica o setor responsável.	0	1	2	3
Rsp_02_3	Verifica se o seu computador está vulnerável a esse ataque.	0	1	2	3
Rsp_03_0	Para que a organização seja segura, convém que todas as responsabilidades e as respectivas atribuições sejam definidas.	Não sei Informar		Não	Sim
Rsp_03_1	Você conhece suas responsabilidades e atribuições relacionadas à Segurança da Informação?			0	1
Rsp_03_2	A sua equipe conhece as suas respectivas responsabilidades e atribuições relacionadas à Segurança da Informação?	0		1	2

Diretriz	Resposta (Reação)			
Definição	Os participantes devem agir em tempo hábil e de maneira cooperativa para prevenir, detectar e responder a incidentes de segurança.			
Descrição	- Os participantes devem reagir prontamente e com um espírito de cooperação aos incidentes de segurança - devem compartilhar suas informações sobre ameaças e vulnerabilidades - devem implementar procedimentos para a rápida e efetiva cooperação a fim de prevenir, detectar e responder a incidentes de segurança			
Id_Item	Item	Categorias		
Rpt_02_0	Suponha que ocorreu um incidente que afeta a segurança da informação, como vírus, interrupção do serviço, perda de dados, invasão. Qual seria a sua atitude em relação a cada uma das partes envolvidas a seguir?	Não Alertaria	Alertaria dependendo da situação	Alertaria Imediatamente
Rpt_02_1	Sua chefia.	0	1	2
Rpt_02_2	Os parceiros internos à organização. (Outros departamentos)	0	1	2
Rpt_02_3	Os parceiros externos à organização. (Organizações parceiras)	0	1	2
Rpt_02_4	O Gestor responsável pela Segurança da Informação.	0	1	2

Id_Item	Item	Categorias				
Rpt_03_0	Você está no seu local de trabalho e percebe a presença de uma pessoa desconhecida e também que não está utilizando uma identificação. Você:	Não	Raramente	Frequentemente	Sempre	N. A.
Rpt_03_1	Comunica ao setor responsável pela segurança?	0	1	2	3	9
Rpt_03_2	Solicita que ela se retire?	0	1	2	3	9
Rpt_03_3	Comunica a sua chefia?	0	1	2	3	9

Rpt_04_0	Supondo que você encontrou um <i>Pendrive</i> no estacionamento nas proximidades da empresa. Você:	Não	Sim
Rpt_04_1	Utiliza o dispositivo em seu equipamento para saber o que contém?	1	0
Rpt_04_2	Pede à equipe de segurança, que avalie o dispositivo?	0	1

Diretriz	Ética					
Definição	Os participantes devem respeitar os interesses legítimos de outros participantes.					
Descrição	- Os participantes devem reconhecer o quanto suas ações ou omissões podem prejudicar os outros. - Devem ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação. - Devem respeitar os interesses legítimos dos outros participantes.					
Id_Item	Item	Categorias				
Etc_01_0	Com que frequência você trata de assuntos relacionados a sua organização nos seguintes ambientes?	Nunca	Raramente	Frequentemente	Sempre	N. A.
Etc_01_1	Dentro de aviões, ônibus, taxi ou elevador.	3	2	1	0	9
Etc_01_2	Em bares ou restaurantes.	3	2	1	0	9
Etc_01_3	Em reuniões sociais.	3	2	1	0	9
Etc_01_4	Na sala de embarque do aeroporto.	3	2	1	0	9
Etc_01_5	No cafezinho.	3	2	1	0	9
Etc_01_6	Em redes sociais. (Facebook, LinkedIn, WhatsApp, chat,...)	3	2	1	0	9
Etc_01_7	Em cabeleireiros, barbeiros ou salão de beleza.	3	2	1	0	9
Etc_01_8	Por telefone fora do ambiente de trabalho.	3	2	1	0	9

Id_Item	Item	Categorias			
Etc_02_0	Você entra na sala de um colega para tratar de um assunto e verifica que ele está ao telefone. Você:	Nunca	Raramente	Frequentemente	Sempre
Etc_02_1	Espera na sala pacientemente enquanto ele está ao telefone?	3	2	1	0
Etc_02_2	Retira-se e aguarda o final do telefonema?	0	1	2	3
Etc_03_0	Suas atividades permitem a você ter acesso a informações confidenciais. Sobre essas informações você costuma:	Nunca	Raramente	Frequentemente	Sempre
Etc_03_1	Conversar com seus colegas?	3	2	1	0
Etc_03_2	Comenta com sua equipe?	3	2	1	0
Etc_03_3	Conversar com seus amigos mais próximos?	3	2	1	0
Etc_03_4	Conversar com seus familiares?	3	2	1	0

Id_Item	Item	Categorias			
Etc_04_0	O seu colega está trabalhando no computador. Você:	Nunca	Raramente	Frequentemente	Sempre
Etc_04_1	Verifica o que ele está fazendo?	3	2	1	0
Etc_04_2	Desvia o olhar enquanto ele digita a senha?	0	1	2	3
Etc_05_0	Com que frequência você costuma:	Nunca	Raramente	Frequentemente	Sempre
Etc_05_1	Emprestar a sua senha para um colega?	3	2	1	0
Etc_05_2	Solicitar a senha de um colega?	3	2	1	0
Etc_05_3	Participar de conversas informais sobre outros colegas?	3	2	1	0
Etc_05_4	Comentar sobre falhas/erros de colegas?	3	2	1	0

Id_Item	Item	Categorias			
Etc_06_0	Com que frequência você costuma alertar os seus colegas sobre a necessidade de:	Nunca	Raramente	Frequentemente	Sempre
Etc_06_1	Desligar o computador quando não estiver em uso?	0	1	2	3
Etc_06_2	Bloquear o computador quando não estiver em sua estação de trabalho?	0	1	2	3
Etc_06_3	Manter a mesa limpa/organizada?	0	1	2	3
Etc_06_4	Proteger os documentos de trabalho de acesso não autorizado?	0	1	2	3

Diretriz	Gestão de Segurança							
Definição	Os participantes devem adotar uma abordagem abrangente para a gestão da segurança.							
Descrição	- Deve ser baseada na avaliação dos riscos. - Deve ser dinâmica e global, de modo a abranger todos os níveis de atividades dos participantes e todos os aspectos de suas operações. - Deve incluir, respostas antecipadas às ameaças emergentes e a prevenção, detecção e resolução dos incidentes, a recuperação dos sistemas, a manutenção contínua, o controle e a auditoria. - As políticas de segurança dos sistemas e redes de informações, as práticas, medidas e procedimentos em matéria de segurança devem ser coordenados e integrados para criar um sistema coerente de segurança. - Os requisitos da gestão de segurança dependem do nível de envolvimento, do papel do participante, dos riscos envolvidos e das características do sistema.							
Id_Item	Item			Categorias				
Gts_01_0	Durante o processo de manuseio dos dados da organização (agenda, cadastros, dados de pessoas, etc.) você executa uma ou mais das seguintes etapas: armazenamento, recuperação ou atualização dos dados. Com que frequência você:			Nunca	Raramente	Frequentemente	Sempre	N. A.
Gts_01_1	Avalia os riscos de danos ou incidentes como perda, roubo, adulteração e acesso indevido aos dados?			0	1	2	3	9
Gts_01_2	Planeja o local e a forma como os dados serão armazenados e acessados, levando-se em consideração a avaliação dos riscos?			0	1	2	3	9

Gts_01_3	Leva em consideração as diretrizes estabelecidas pela sua organização no planejamento?	0	1	2	3	9
Gts_01_4	Executa os processos conforme planejado?	0	1	2	3	9
Gts_01_5	Avalia se os procedimentos adotados estão atendendo às necessidades de segurança?	0	1	2	3	9
Gts_01_6	Executa as modificações necessárias para adequar às novas necessidades?	0	1	2	3	9

Id_Item	Item	Categorias			
Gts_02_00	Para a melhor gestão da segurança da informação é recomendado que a organização tenha um comitê ou grupo gestor da segurança da informação. Com respeito a essa afirmação	Não sei Informar	Não	Sim	
Gts_02_1	A sua organização possui um grupo gestor da S.I.?	0	1	2	
Gts_02_2	Você acha necessário ter um grupo gestor na sua organização?	0	1	2	

Diretriz	Democracia			
Definição	A segurança dos sistemas e redes de informação deve ser compatível com os valores essenciais de uma sociedade democrática.			
Descrição	- Os participantes devem respeitar os valores, a liberdade de troca de ideias, pensamentos, o livre fluxo de informações, a confidencialidade da informação e da comunicação, a proteção adequada dos dados pessoais, a abertura e a transparência. - Os participantes devem respeitar e reconhecer a liderança.			
Id_Item	Item	Categorias		
Dmc_01_0	O líder de uma equipe ou organização deve ser capaz de comandar pessoas, atrair seguidores, influenciar e motivar positivamente o comportamento do grupo.	Não	Sim	N.A. ou Não tenho Chefe
Dmc_01_1	Na sua opinião, o seu chefe é um líder?	0	1	9
Dmc_01_2	O seu chefe motiva ou incentiva um comportamento a favor da segurança da informação?	0	1	9
Dmc_01_3	Você se sente seguro(a) com a liderança do seu chefe em relação à segurança da informação?	0	1	9

Id_Item	Item	Categorias				
Dmc_02_0	Durante um processo de tomada de decisão que tem como consequência mudanças de hábitos e comportamentos da sua equipe ou grupo de trabalho, o seu chefe:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Dmc_02_1	Impõe as suas decisões sem ouvir a opinião dos colegas?	3	2	1	0	9
Dmc_02_2	Estimula os colegas a emitirem opiniões, promove um ambiente participativo?	0	1	2	3	9
Dmc_02_3	Dá total liberdade aos colegas para decidirem e simplesmente homologa o que foi decidido?	3	2	1	0	9

Id_Item	Item	Categorias			
Dmc_03_0	Sobre o seu ambiente de trabalho.	Nunca	Raramente	Frequentemente	Sempre
Dmc_03_1	Você se sente confortável em emitir suas opiniões?	0	1	2	3
Dmc_03_2	Você aceita a opinião dos seus colegas mesmo que elas entrem em conflito com as suas?	0	1	2	3
Dmc_03_3	A sua equipe aceita a divergências de posicionamentos?	0	1	2	3

Id_Item	Item	Categorias				
Dmc_04_0	O setor responsável pelo controle de acesso aos sistemas da organização resolve modificar as regras de criação e a periodicidade das senhas.	Nunca	Raramente	Frequentemente	Sempre	N. A.
Dmc_04_1	Você aceita as regras sem questionamentos?	0	1	2	3	9
Dmc_04_2	A sua equipe aceita as regras sem questionamentos?	0	1	2	3	9

Id_Item	Item	Categorias	
Dmc_05_0	Quanto a sua percepção da segurança da informação na sua organização:	Não	Sim
Dmc_05_1	Você se sente seguro(a) quanto a proteção dos seus dados pessoais na organização?	0	1
Dmc_05_2	Você se sente seguro(a) com relação à confidencialidade das informações da organização?	0	1

Id_Item	Item	Categorias			
Dmc_06_0	Como você avalia a sua organização no seguinte aspecto:	Não existe	Precária	Suficiente	Boa
Dmc_06_1	Comunicação da chefia?	0	1	2	3
Dmc_06_2	Comunicação entre colegas?	0	1	2	3
Dmc_06_3	Transparência administrativa?	0	1	2	3

Diretriz	Avaliação de Risco					
Definição	Os participantes devem realizar avaliações de risco.					
Descrição	- As avaliações devem ser suficientemente amplas para abranger o conjunto dos principais fatores internos e externos, tais como tecnologia, fatores físicos e humanos, políticas e serviços de terceiros que influenciam na segurança da informação.					
Id_Item	Item	Categorias				
Rsc_01_0	Com respeito a cópia de segurança dos seus arquivos profissionais, com que frequência você realiza as seguintes atividades?	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_01_1	Cópia de segurança em mídias externas. (CD, DVD, <i>Storage</i> , <i>Pendrive</i> ,...)	0	1	2	3	9
Rsc_01_2	Cópia de segurança no mesmo computador de trabalho.	3	2	1	0	9
Rsc_01_3	Verifica se as copias de segurança estão atualizadas.	0	1	2	3	9

Id_Item	Item	Categorias				
Rsc_02_0	Instalação de Software (aplicativos):	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_02_1	Você costuma instalar software ou aplicativos de seu interesse no seu computador de trabalho?	3	2	1	0	9
Rsc_02_2	Você pede autorização para instalar software ou aplicativos de seu interesse no seu computador de trabalho?	0	1	2	3	9
Rsc_03_0	Enquanto você está na sua posição de trabalho, com que frequência você costuma:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_03_1	Fumar?	3	2	1	0	9
Rsc_03_2	Beber? (Água, Sucos, etc)	3	2	1	0	9
Rsc_03_3	Alimentar-se?	3	2	1	0	9

Id_Item	Item	Categorias				
Rsc_04_0	Quando você recebe um e-mail com arquivo anexo, com que frequência você costuma:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_04_1	Abrir o anexo?	3	2	1	0	9
Rsc_04_2	Passar o antivírus antes de abrir o anexo?	0	1	2	3	9
Rsc_04_3	Verificar a procedência do e-mail antes de abrir o anexo?	0	1	2	3	9
Rsc_05_0	Quando você recebe um endereço de sítio da Internet (link), com que frequência você:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_05_1	Acessa o link independente de quem enviou?	3	2	1	0	9
Rsc_05_2	Acessa o link se vier de remetente conhecido?	3	2	1	0	9
Rsc_05_3	Verifica se o link é seguro?	0	1	2	3	9

Id_Item	Item	Categorias				
Rsc_06_0	Ao receber uma mídia (CD, DVD, <i>Pendrive</i> ,...) com que frequência você:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_06_1	Abre a mídia, independente de quem a enviou?	3	2	1	0	9
Rsc_06_2	Executa os programas contidos na mídia?	3	2	1	0	9
Rsc_06_3	Passa o antivírus antes de abrir ou executar programas da mídia?	0	1	2	3	9
Rsc_07_0	Uso do e-mail corporativo.	Não	Sim	N.A.		
Rsc_07_1	Você utiliza o e-mail da organização para receber mensagens pessoais?	1	0	9		
Rsc_07_2	Você utiliza o e-mail da organização para enviar mensagens pessoais?	1	0	9		
Rsc_07_3	Você divulga o e-mail da organização para os seus contatos pessoais?	1	0	9		

Id_Item	Item	Categorias				
Rsc_08_0	Ao receber um e-mail com conteúdos tipo <i>SPAM</i> (propagandas, anúncios, ...). Com que frequência você:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_08_1	Abre o e-mail para ver se o conteúdo interessa?	3	2	1	0	9
Rsc_08_2	Denuncia como <i>SPAM</i> e/ou bloqueia o remetente?	0	1	2	3	9
Rsc_08_3	Repassa ou reencaminha o e-mail?	3	2	1	0	
Rsc_09_0	Com que frequência você costuma utilizar o computador da organização para acessar:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_09_1	Suas Redes sociais (Facebook, linkedin, ...)?	3	2	1	0	9
Rsc_09_2	Contas externas de e-mail pessoais?	3	2	1	0	9
Rsc_09_3	Sítios de compras?	3	2	1	0	9
Rsc_09_4	Jogos?	3	2	1	0	9
Rsc_09_5	Seu Banco (Caixa, Banco do Brasil, ...)?	3	2	1	0	9

Id_Item	Item	Categorias				
Rsc_10_0	Supondo que você não está presente no seu local de trabalho e o seu colega necessita de um arquivo que está no seu computador, você:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_10_1	Passa a sua senha de acesso para que ele possa pegar o arquivo?	3	2	1	0	9
Rsc_10_2	Comunica a sua senha ao seu chefe para que ele se responsabilize pelo acesso?	0	1	2	3	9
Rsc_11_0	No momento da composição da sua senha de acesso, quais dos elementos a seguir você costuma utiliza?	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_11_1	Nomes ou apelidos.	3	2	1	0	9
Rsc_11_2	Datas ou parte de datas.	3	2	1	0	9
Rsc_11_3	Números, letras e caracteres especiais misturados.	0	1	2	3	9
Rsc_11_4	Uma senha padrão.	3	2	1	0	9

Id_Item	Item	Categorias				
Rsc_12_0	Independente do equipamento ser pessoal ou profissional, você tem por hábito:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_12_1	Trocar a sua senha de acesso?	0	1	2	3	
Rsc_12_2	Criptografar os dados importantes?	0	1	2	3	9
Rsc_12_3	Acessar redes sem fio abertas (WIFI sem senha) em locais públicos, tais como aeroportos e restaurantes?	3	2	1	0	9
Rsc_12_4	Guardar ou fixar a senha de acesso no próprio equipamento? (Computador, Celular.)	3	2	1	0	
Rsc_12_5	Bloquear o computador ao se afastar dele por algum motivo?	0	1	2	3	
Rsc_12_6	Limpar, higienizar o seu equipamento de trabalho?	0	1	2	3	
Rsc_13_0	Ao acessar uma página na Internet você:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_13_1	Verifica se o sítio é seguro?	0	1	2	3	9
Rsc_13_2	Verifica se a rede é segura?	0	1	2	3	9

Id_Item	Item	Categorias				
Rsc_14_0	Independente da atividade que está fazendo, ao utilizar a sua senha você:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_14_1	Verifica se alguém está te observando?	0	1	2	3	9
Rsc_14_2	Verifica se está sendo filmado?	0	1	2	3	9
Rsc_14_3	Verifica se o dispositivo que está utilizando está em bom estado de conservação?	0	1	2	3	9
Rsc_15_0	Durante o processo de instalação de um aplicativo você:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Rsc_15_1	Lê a licença de uso do aplicativo?	0	1	2	3	9
Rsc_15_2	Procura saber a procedência do aplicativo?	0	1	2	3	9

Id_Item	Item	Categorias				
Rsc_16_0	Uma questão importante no processo da segurança da informação é o descarte de mídias. (CD, DVD, Disquete, fita magnética, papel, etc.) Ao descartar uma mídia, com que frequência você realiza os procedimentos a seguir?	Nunca	Raramente	Frequentemente	Sempre	N.A.
Rsc_16_1	Confirma o conteúdo da mídia antes de descartar.	0	1	2	3	9
Rsc_16_2	Destroi a mídia.	0	1	2	3	9
Rsc_16_3	Registra o descarte ou a baixa da mídia.	0	1	2	3	9
Rsc_16_4	Verifica se a mídia está em conformidade com os requisitos para o seu descarte.	0	1	2	3	9
Rsc_17_0	Com respeito ao uso do crachá	Nunca	Raramente	Frequentemente	Sempre	NA
Rsc_17_1	Utiliza o seu crachá de identificação em local visível?	0	1	2	3	9
Rsc_17_2	Verifica se as pessoas que passam por você estão utilizando o crachá de identificação?	0	1	2	3	9

Diretriz	Projeto de Segurança e Implementação		
Definição	Os participantes devem integrar a segurança como um elemento essencial dos sistemas e redes de informação.		
Descrição	- Os participantes devem preocupar-se com a criação e adoção de salvaguardas e soluções para evitar ou limitar o dano potencial de ameaças e vulnerabilidades identificadas.		
Id_Item	Item	Categorias	
Prj_01_0	Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes..	Não sei informar ou Não Implementada	Parcialmente ou totalmente Implementada
Prj_01_1	A política de segurança da informação na sua organização está em que estágio?	0	1

Id_Item	Item	Categorias				
Prj_02_0	Convém que a segurança da informação seja considerada em todas as fases do projeto, independentemente do tipo do projeto. Com que frequência a segurança da informação é considerada na fase de:	Nunca	Raramente	Frequentemente	Sempre	N. A.
Prj_02_1	Definição e elaboração do projeto.	0	1	2	3	9
Prj_02_2	Execução do projeto.	0	1	2	3	9
Prj_02_3	Gerenciamento do projeto.	0	1	2	3	9

Id_Item	Item	Categorias				
Prj_03_0	Durante o ciclo de um projeto ou trabalho, com que frequência você e sua equipe realizam as atividades a seguir?	Nunca	Raramente	Frequentemente	Sempre	N. A.
Prj_03_1	Antes de iniciarem um novo trabalho ou projeto, fazem um levantamento dos riscos de possíveis incidentes que possam prejudicar o andamento ou a organização.	0	1	2	3	9
Prj_03_2	Durante o decorrer das atividades, reavaliam os procedimentos em busca de falhas ou possíveis incidentes.	0	1	2	3	9
Prj_03_3	Após a conclusão da atividade, projeto ou trabalho, formalizam por meio de documento as intercorrências para uso futuro.	0	1	2	3	9
Prj_03_4	Verificam se o trabalho ou projeto está em conformidade no tocante às recomendações.	0	1	2	3	9

Diretriz	Reavaliação				
Definição	Os participantes devem analisar e reavaliar a segurança dos sistemas e redes de informação, e fazer as modificações necessárias nas políticas, práticas, medidas e procedimentos de segurança.				
Descrição	- Todos os participantes devem continuamente rever, reavaliar e modificar todos os aspectos da segurança para lidar com esses riscos que estão em evolução.				
Id_Item	Item	Categorias			
Rvl_01_0	Convém que as políticas de segurança da informação sejam analisadas criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.	Nunca	Raramente	Frequentemente	Sempre
Rvl_01_1	Com que frequência você ou sua equipe revisa as políticas de segurança da informação da sua organização?	0	1	2	3
Rvl_01_2	Você é convidado(a) a participar da reavaliação das políticas de segurança da Informação?	0	1	2	3

Id_Item	Item	Categorias				
Rvl_02_0	A Segurança da Informação é uma área que requer uma reavaliação constante.	Nunca	Raramente	Frequentemente	Sempre	Desconheço
Rvl_02_1	Com que frequência você reavalia as suas atitudes com respeito a segurança da informação?	0	1	2	3	
Rvl_02_2	Na sua opinião qual seria a frequência adequada para um funcionário reavaliar os seus hábitos com respeito a S.I.?	0	1	2	3	
Rvl_02_3	Com que frequência a sua organização promove uma reavaliação dos procedimentos de segurança da informação?	0	1	2	3	9

APÊNDICE B – Itens Recategorizados

Quadro 6 - Itens Recategorizados

Cod. Item	Item	Recodificação
Csc_03_0	Em sua opinião, qual seria o impacto na sua organização caso ocorra um dos incidentes a seguir?	
Csc_03_1	Perda dos dados e informações	0 – leve 1 - severa
Csc_03_2	Acesso indevido aos dados e informações	0 – leve 1 - severa
Csc_03_3	Adulteração dos dados	0 – leve 1 - severa
Etc_01_3	Com que frequência você trata de assuntos relacionados à sua organização nos seguintes ambientes? Em reuniões sociais.	0 – sempre 1 – às vezes 2 – nunca
Etc_05_1	Com que frequência você costuma: emprestar a sua senha para um colega?	0 – sempre 1 – às vezes 2 – nunca
Dmc_06_1	Como você avalia a sua organização nos seguintes aspectos: comunicação com a chefia	0 – precária 1 – suficiente 2 - boa
Rsc_08_	Ao receber um e-mail com conteúdos tipo spam (propagandas, anúncios, ...). Com que frequência você:	
Rsc_08_1	Abre o e-mail para ver se o conteúdo interessa?	0 – sempre 1 – às vezes 2 – nunca
Rsc_08_3	Repassa ou reencaminha o e-mail?	0 – sempre 1 – às vezes 2 – nunca
Rsc_09_4	Com que frequência você costuma utilizar o computador da organização para acessar: jogar	0 – sempre 1 – às vezes 2 – nunca
Csc_03_0	Em sua opinião, qual seria o impacto na sua organização caso ocorra um dos incidentes a seguir?	
Csc_03_1	A perda dos dados e informações	0-nenhum ou leve 1-severa
Csc_03_2	Acesso indevido aos dados e informações	0-nenhum ou leve 1-severa
Csc_03_3	Adulteração dos dados	0-nenhum ou

		leve 1-severa
Csc_03_4	Divulgação não autorizada das informações	0-nenhum ou leve 1-severa
Csc_03_5	Interrupção ou indisponibilidade dos serviços (Internet, acessos remotos, banco de dados, etc)	0-nenhum ou leve 1-severa
Csc_03_6	Quebra do sigilo da informação	0-nenhum ou leve 1-severa
Csc_03_7	Furto dos dados e informações	0-nenhum ou leve 1-severa
Csc_06_0	A classificação da informação é uma etapa muito importante para a segurança da informação. Sobre a classificação da informação na sua organização.	
Csc_06_1	Você sabe se sua organização tem os procedimentos e diretrizes para classificação da informação implementados?	0 - não sabe 1 – sabe
Dmc_02_0	Durante um processo de tomada de decisão que tem como consequência mudanças de hábitos e comportamentos da sua equipe ou grupo de trabalho. O seu chefe:	
Dmc_02_1	Impõe as suas decisões sem ouvir a opinião dos colegas?	0-sempre 1-às vezes 2- raramente
Dmc_02_2	Estimula os colegas a emitirem opiniões, promove um ambiente participativo?	0-nunca 1-às vezes 2-sempre
Dmc_02_3	Dá total liberdade aos colegas para decidirem e simplesmente homologa o que foi decidido.	0-sempre 1-às vezes 2-nunca
Dmc_03_0	Sobre o seu ambiente de trabalho.	
Dmc_03_1	Você se sente confortável em emitir suas opiniões?	0-nunca 1-às vezes 2-sempre
Dmc_03_2	Você aceita a opinião dos seus colegas mesmo que elas entrem em conflito com as suas?	0-nunca 1-às vezes 2-sempre
Dmc_03_3	A sua equipe aceita a divergências de posicionamentos?	0-nunca 1-às vezes 2-sempre

Dmc_04_0	O setor responsável pelo controle de acesso aos sistemas da organização resolve modificar as regras de criação e a periodicidade das senhas. Você:	
Dmc_04_1	Você aceita as regras sem questionamentos?	0-nunca 1-às vezes 2-sempre
Dmc_04_2	A sua equipe aceita as regras sem questionamento?	0-nunca 1-às vezes 2-sempre
Dmc_06_0	Como você avalia a sua organização nos seguintes aspectos:	
Dmc_06_1	Comunicação da chefia?	0-não existe ou precária 1-suficiente 2-bom
Dmc_06_2	Comunicação entre colegas?	0-não existe ou precária 1-suficiente 2-bom
Dmc_06_3	Transparência administrativa?	0-não existe ou precária 1-suficiente 2-bom
Etc_01_0	com que frequência você trata de assuntos relacionados à sua organização nos seguintes ambientes?	
Etc_01_1	Dentro de aviões, ônibus, taxi ou elevador.	0-nunca 1-às vezes 2-sempre
Etc_01_2	Em bares ou restaurantes.	0-nunca 1-às vezes 2-sempre
Etc_01_3	Em reuniões sociais.	0-nunca 1-às vezes 2-sempre
Etc_01_4	Na sala de embarque do aeroporto.	0-nunca 1-às vezes 2-sempre
Etc_01_5	No cafezinho.	0-nunca 1-às vezes 2-sempre
Etc_01_6	Em redes sociais (FACEBOOK, LINKEDIN, WHATSAPP, CHAT,...)	0-nunca 1-às vezes 2-sempre

Etc_01_7	Em cabeleireiros, barbeiros ou salão de beleza.	0-nunca 1-às vezes 2-sempre
Etc_01_8	Por telefone fora do ambiente de trabalho.	0-nunca 1-às vezes 2-sempre
Etc_02_0	Você entra na sala de um colega para tratar de um assunto e verifica que ele está ao telefone. Você:	
Etc_02_1	Espera na sala pacientemente enquanto ele está ao telefone?	0-nunca 1-às vezes 2-sempre
Etc_02_2	Retira-se e aguarda o final do telefonema?	0-nunca 1-às vezes 2-sempre
Etc_03_0	Suas atividades permitem a você ter acesso a informações confidenciais. Sobre essas informações você costuma:	
Etc_03_1	Comenta com seus colegas?	0- sempre 1-às vezes 2-nunca
Etc_03_2	Comenta com sua equipe?	0- sempre 1-às vezes 2-nunca
Etc_03_3	Comenta com seus amigos mais próximos?	0- sempre 1-às vezes 2-nunca
Etc_03_4	Comenta com seus familiares?	0- sempre 1-às vezes 2-nunca
Etc_04_0	O seu colega está trabalhando no computador. Você:	
Etc_04_1	Verifica o que ele está fazendo?	0- sempre 1-às vezes 2-nunca
Etc_04_2	Desvia o olhar enquanto ele digita a senha	0-nunca 1-às vezes 2-sempre
Etc_05_0	Com que frequência você costuma:	
Etc_05_1	Emprestar a sua senha para um colega?	0-sempre 1-raramente 2-nunca
Etc_05_2	Solicitar a senha de um colega?	0-sempre 1-raramente 2-nunca

Etc_05_3	Participar de conversas informais sobre outros colegas?	0-sempre 1-raramente 2-nunca
Etc_05_4	Comentar sobre falhas/erros de colegas?	0-sempre 1-raramente 2-nunca
Etc_06_0	Com que frequência você costuma alertar os seus colegas sobre a necessidade de:	
Etc_06_2	Bloquear o computador quando sai da sala?	0 -nunca 1 -às vezes 2 - sempre
Etc_06_3	Manter a mesa limpa/organizada?	0 -nunca 1 -às vezes 2 - sempre
Gts_01_0	Durante o processo de manuseio dos dados da organização (agenda, cadastros, dados de pessoas, etc.) Você executa uma ou mais das seguintes etapas: armazenamento, recuperação ou atualização dos dados. Com que frequência você realiza as seguintes atividades?	
Gts_01_3	Leva em consideração as diretrizes estabelecidas pela sua organização no planejamento.	0 -nunca 1 -às vezes 2 - sempre
Gts_02_0	Para a melhor gestão da segurança da informação é recomendado que a organização tenha um comitê ou grupo gestor da segurança da informação. Com respeito a essa afirmação	
Gts_02_1	A sua organização possui um grupo gestor da s.i.?	0 – não sei informar ou não tem 1 – sim, tem
Gts_02_2	Você acha necessário ter um grupo gestor na sua organização	0 – não sei informar ou não 1 – sim, é
Prj_01_0	Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.	
Prj_01_1	A política de segurança da informação na sua organização está em que estágio?	0 – não sei informar ou não implementada 1 –parcialmente ou totalmente implementada
Prj_02_0	Convém que a segurança da informação seja considerada em todas as fases do projeto, independentemente do tipo do projeto. Com que frequência a segurança da informação é considerada na fase de:	

Prj_02_1	Definição e elaboração do projeto.	0 -nunca 1 -às vezes 2 - sempre
Prj_03_0	Durante o ciclo de um projeto ou trabalho, com que frequência você e sua equipe realizam as atividades a seguir?	
Prj_03_4	Verificam se o trabalho ou projeto está em conformidade no tocante às recomendações.	0 -nunca 1 -às vezes 2 - sempre
Rpt_03_0	Você está no seu local de trabalho e percebe a presença de uma pessoa desconhecida e também que não está utilizando uma identificação. Você:	
Rpt_03_1	Comunica a segurança?	0 -nunca 1 -às vezes 2 - sempre
Rpt_03_2	Solicita que ela se retire?	0 -nunca 1 -às vezes 2 - sempre
Rpt_03_3	Comunica a sua chefia?	0 -nunca 1 -às vezes 2 - sempre
Rsc_02_0	Instalação de software (aplicativos)	
Rsc_02_1	Você costuma instalar software ou aplicativos de seu interesse no seu computador de trabalho?	2 -nunca 1 -às vezes 0 - sempre
Rsc_02_2	Você pede autorização para instalar software ou aplicativos de seu interesse no seu computador de trabalho?	0 -nunca 1 -às vezes 2 - sempre
Rsc_03_0	Enquanto você está na sua posição de trabalho, com que frequência você costuma fazer as seguintes atividades?	
Rsc_03_2	Beber	2 -nunca 1 -às vezes 0 - sempre
Rsc_04_0	Quando você recebe um e-mail com arquivo anexo, com que frequência você costuma:	
Rsc_04_1	Abrir o anexo.	2 -nunca 1 -às vezes 0 - sempre
Rsc_04_2	Passar o antivírus antes de abrir o anexo.	0 -nunca 1 -às vezes 2 - sempre
Rsc_04_3	Verificar a procedência do e-mail antes de abrir o anexo	0 -nunca 1 -às vezes 2 - sempre

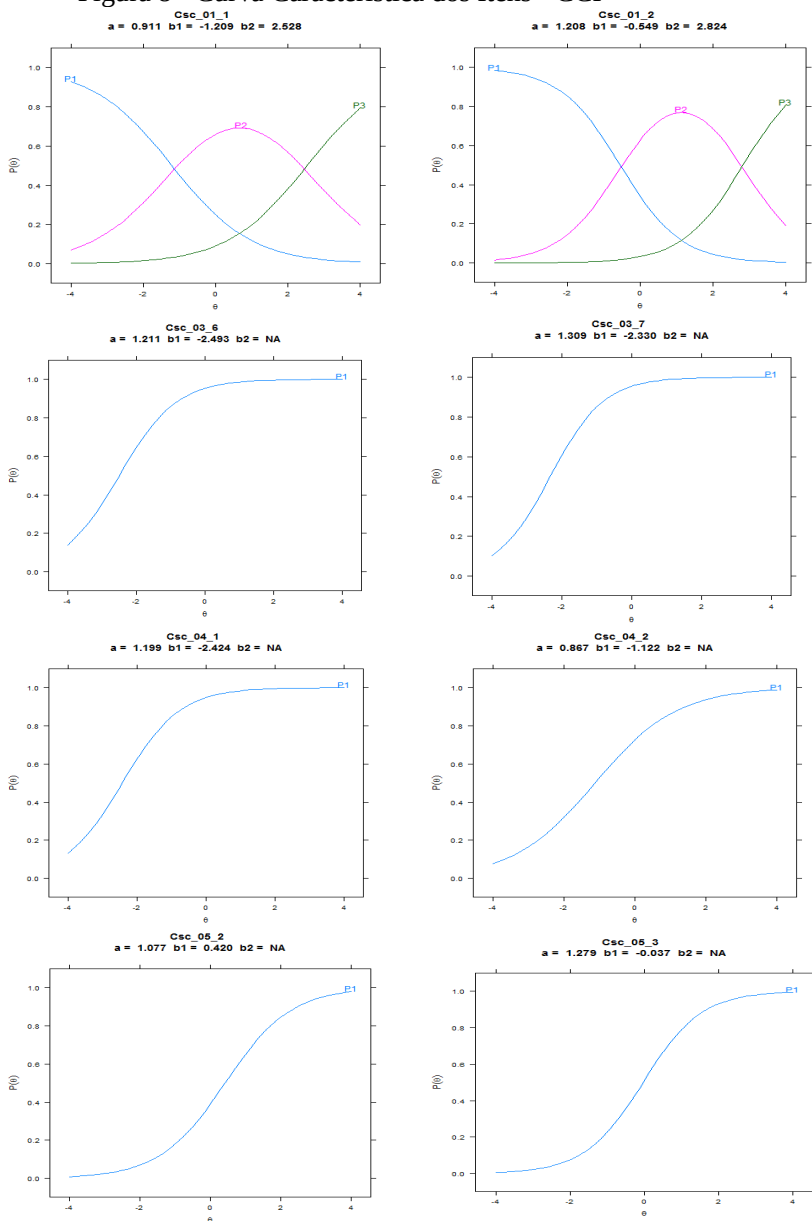
Rsc_05_0	Quando você recebe um endereço de sítio da Internet (link), com que frequência você:	
Rsc_05_1	Acessa o link independente de quem enviou?	2 -nunca 1 -às vezes 0 - sempre
Rsc_05_2	Acessa o link se vier de remetente conhecido?	2 -nunca 1 -às vezes 0 - sempre
Rsc_05_3	Verifica se o link é seguro?	0-nunca 1 - às vezes 2-sempre
Rsc_06_0	Ao receber uma mídia (cd, dvd, <i>pendrive</i> ,...) Com que frequência você:	
Rsc_06_1	Abre a mídia, independente de quem enviou?	0-nunca 1-às vezes 2-sempre
Rsc_06_2	Executa os programas contidos na mídia?	0-nunca 1-às vezes 2-sempre
Rsc_08_0	Ao receber um e-mail com conteúdos tipo <i>spam</i> (propagandas, anúncios, ...). Com que frequência você:	
Rsc_08_1	Abre o e-mail para ver se o conteúdo interessa?	0-sempre 1-às vezes 2-nunca
Rsc_08_3	Repassa ou reencaminha o e-mail?	0-sempre 1-às vezes 2-nunca
Rsc_09_0	Com que frequência você costuma utilizar o computador da organização para acessar:	
Rsc_09_1	Suas redes sociais (FACEBOOK, LINKEDIN)?	0-sempre 1-às vezes 2-nunca
Rsc_09_3	Sítios de compras?	0-sempre 1-às vezes 2-nunca
Rsc_09_4	Jogos?	0-sempre 1-às vezes 2-nunca
Rsc_10_0	Supondo que você não está presente no seu local de trabalho e o seu colega necessita de um arquivo que está no seu computador. Você:	
Rsc_10_1	Passa a sua senha de acesso para <i>que ele possa</i>	0-sempre

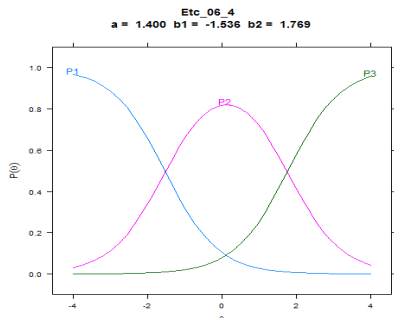
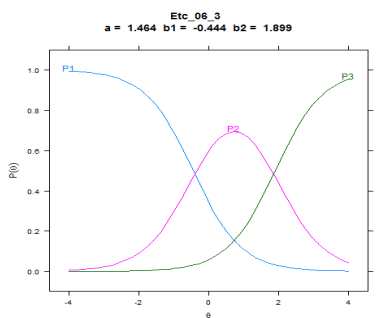
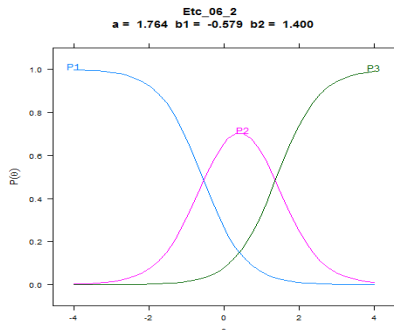
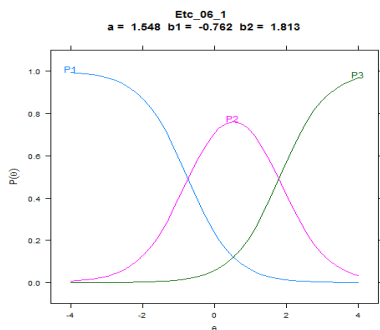
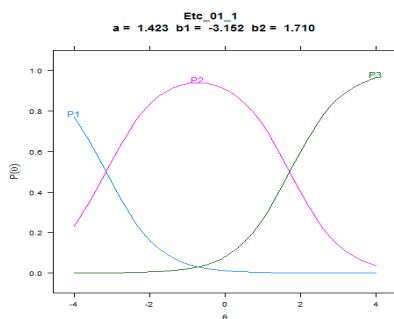
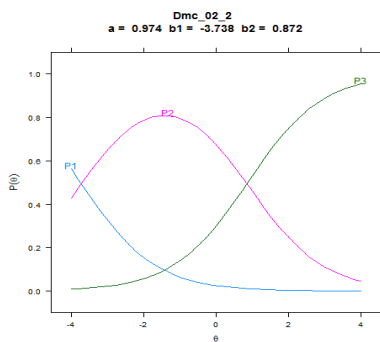
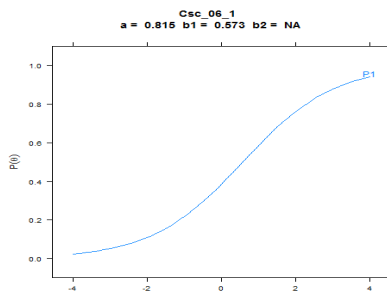
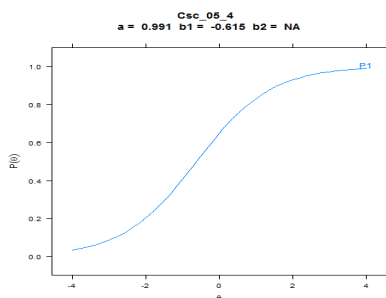
	<i>pegar o arquivo?</i>	1-às vezes 2-nunca
Rsc_10_2	Comunica a sua senha ao seu chefe para que ele se responsabilize pelo acesso?	0-sempre 1-às vezes 2-nunca
Rsc_12_0	Independente do equipamento ser pessoal ou profissional, você tem por hábito:	
Rsc_12_3	Acessar redes sem fio abertas (wifi sem senha) em locais públicos como: (aeroportos, restaurantes, ...)	0-sempre 1-às vezes 2-nunca
Rsc_12_4	Guardar ou fixar a senha de acesso no próprio equipamento. (computador, celular, ..)	0-sempre 1-às vezes 2-nunca
Rsc_15_0	Durante o processo de instalação de um aplicativo você:	
Rsc_15_1	Lê a licença de uso do aplicativo?	0-nunca 1-às vezes 2-sempre
Rsc_17_0	Com respeito ao uso do crachá	
Rsc_17_1	Utiliza o seu crachá de identificação em local visível?	0-nunca 1-às vezes 2-sempre
Rvl_02_0	A segurança da informação é uma área que requer uma reavaliação constante.	
Rvl_02_2	Na sua opinião qual seria a frequência adequada para um funcionário reavaliar os seus hábitos com respeito a s.i.?	0-nunca 1-às vezes 2-sempre

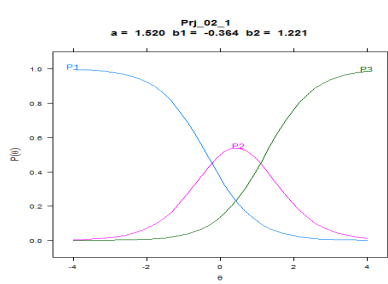
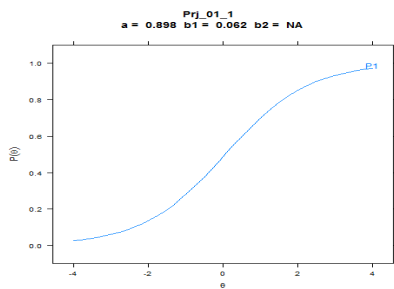
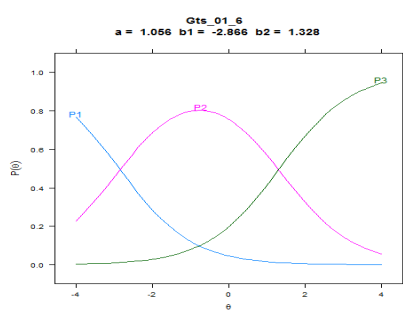
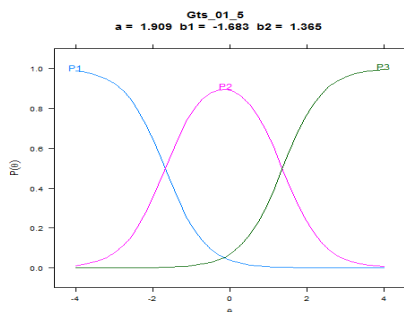
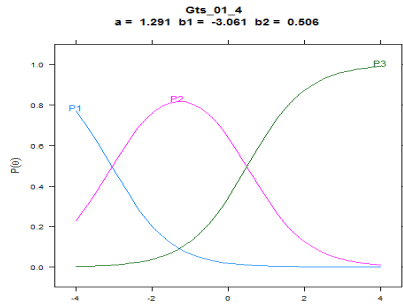
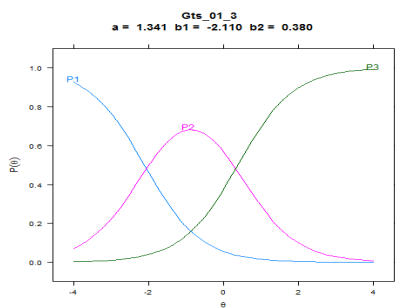
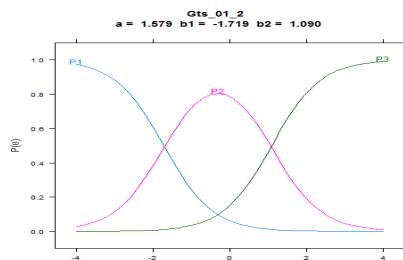
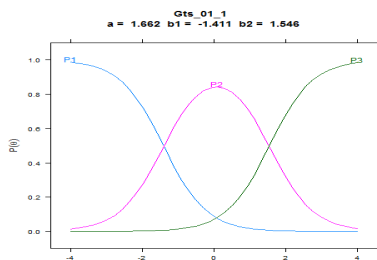
Fonte: Elaborado pelo autor (2017).

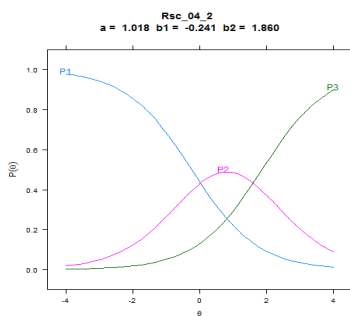
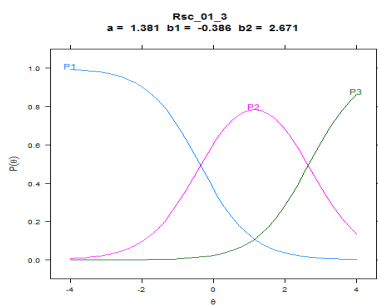
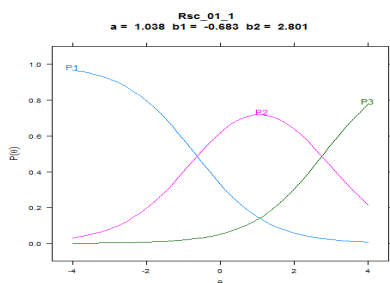
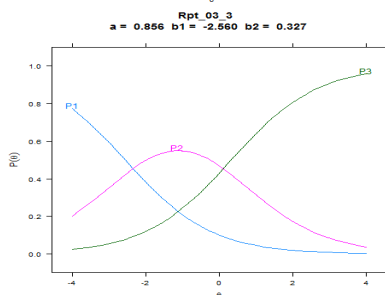
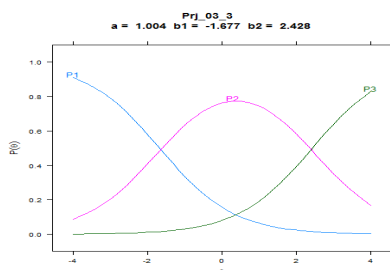
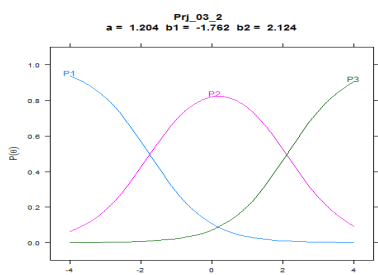
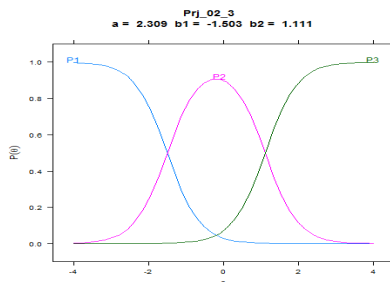
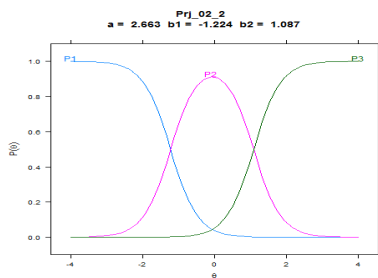
APÊNDICE C – Gráfico dos itens

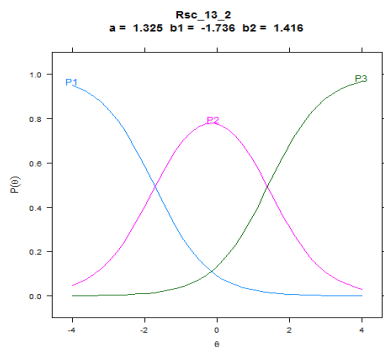
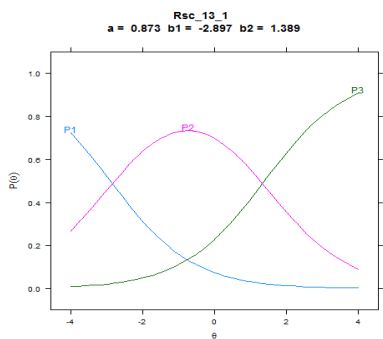
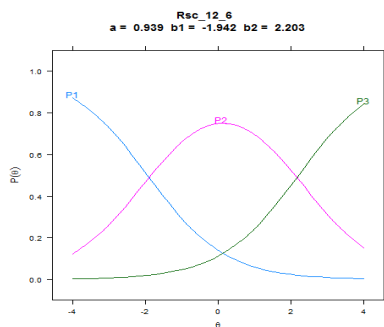
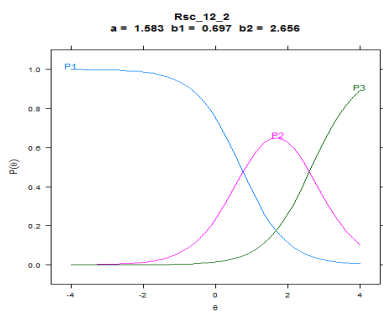
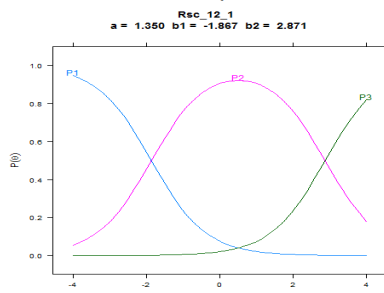
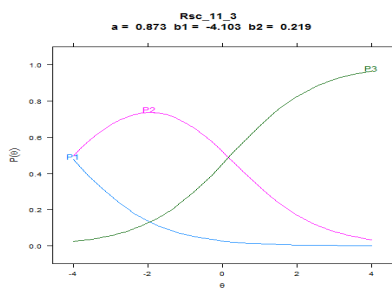
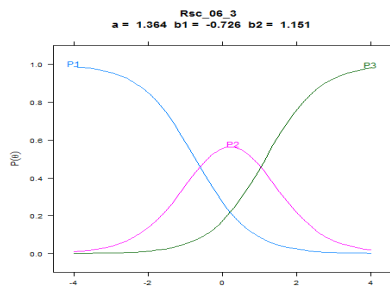
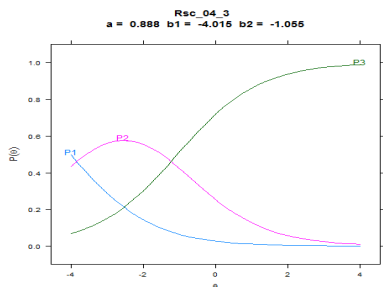
Figura 8 - Curva Característica dos Itens - CCI

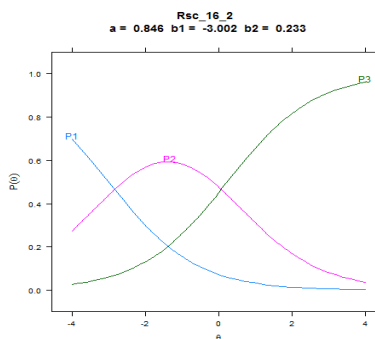
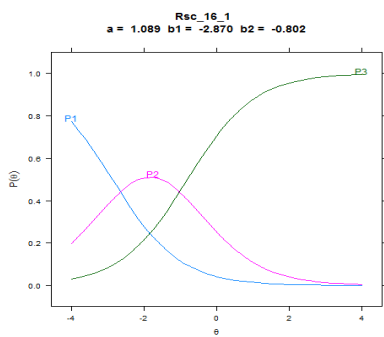
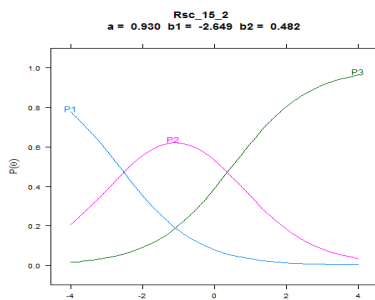
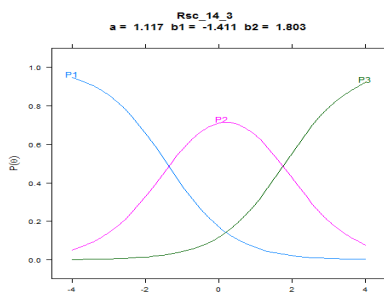
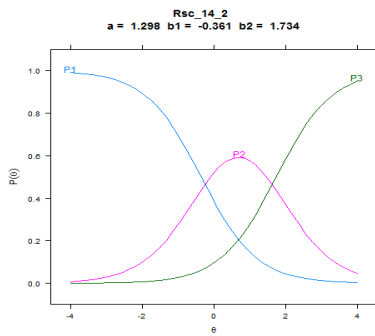
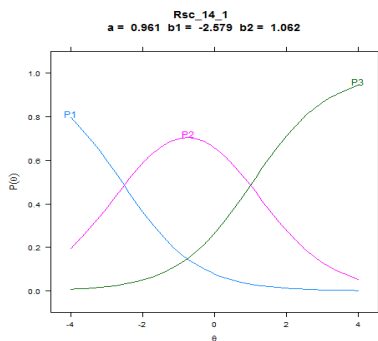


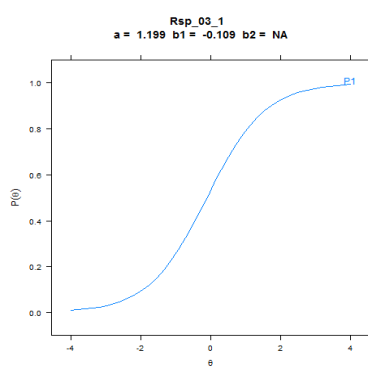
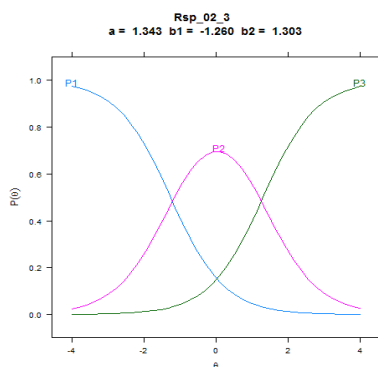
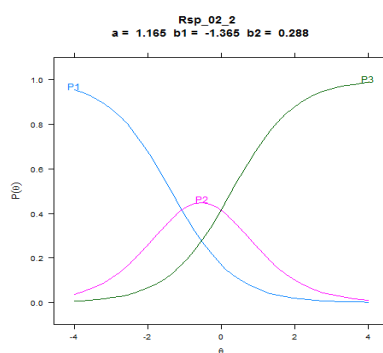
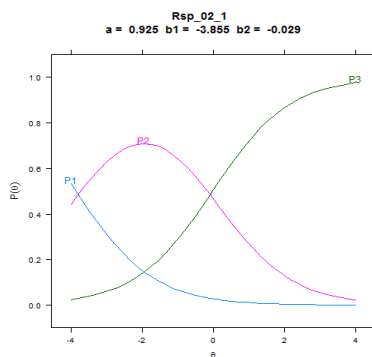
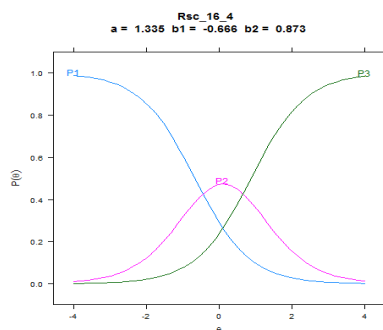
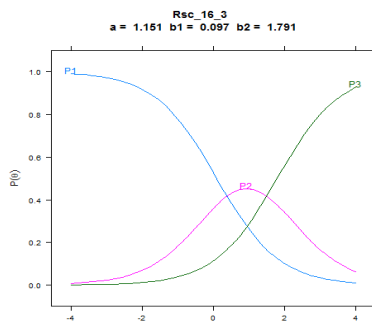


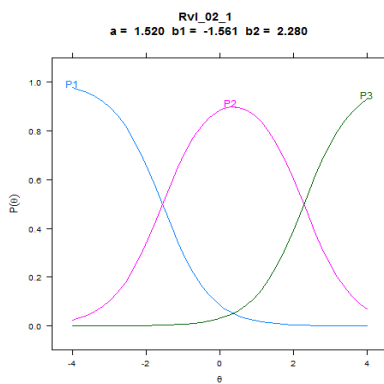
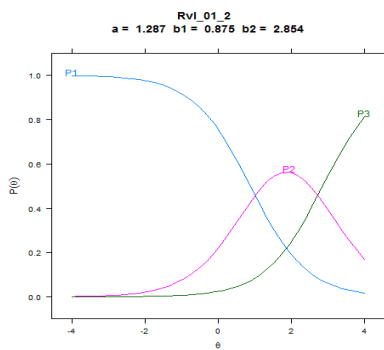
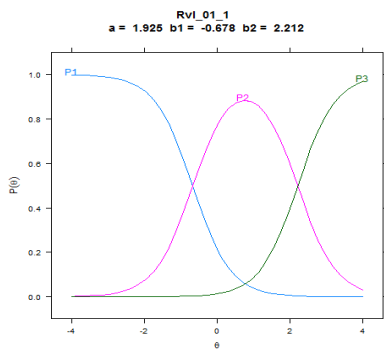












APENDICE D – Parâmetros Transformados

Tabela 13 - Parâmetros após transformação

item	a	b1	b2	Descrição do Item
Csc_01_1	0,085	87,033	126,989	Com que frequência você verifica se o antivírus está atualizado?
Csc_01_2	0,112	94,058	130,924	Com que frequência você verifica o histórico do antivírus?
Csc_03_6	0,107	71,897		Quebra do sigilo da informação
Csc_03_7	0,121	74,544		Furto dos dados e informações
Csc_04_1	0,113	74,061		Sabe qual é o sistema operacional do seu equipamento?
Csc_04_2	0,078	87,821		Sabe qual a versão do sistema operacional do seu computador?
Csc_05_2	0,098	104,692		Sabe qual é a quantidade de memória RAM?
Csc_05_3	0,115	99,459		Sabe qual a capacidade de armazenamento do disco?
Csc_05_4	0,089	93,105		Sabe o tipo de conexão do seu computador com a rede?
Csc_06_1	0,075	106,484		Você sabe se sua organização tem os procedimentos e diretrizes para classificação da informação implementados?
Rsp_02_1	0,085	60,288	99,879	Alerta os colegas de equipe
Rsp_02_2	0,107	85,482	103,294	Comunica o setor responsável.
Rsp_02_3	0,122	86,157	114,533	Verifica se o seu computador está vulnerável a esse ataque.
Rsp_03_1	0,106	98,730		Você conhece suas responsabilidades e atribuições relacionadas à S.I.?

Continuação				
item	a	b1	b2	Descrição do Item
Rpt_01_3	0,092	81,734	127,293	Após a conclusão da atividade, projeto ou trabalho, formalizam por meio de documento as intercorrências para uso futuro.
Rpt_03_3	0,077	71,821	103,655	Comunica a sua chefia?
Etc_01_1	0,120	63,068	119,633	Com que frequência você trata de assuntos relacionados à sua organização em ambientes como (Dentro de aviões, ônibus, taxi, elevador, Sala de cafezinho, Redes Sociais, Bares,...)?
Etc_06_1	0,142	91,597	119,803	Desligar o computador quando não estiver em uso?
Etc_06_2	0,160	93,786	115,602	Bloquear o computador quando sai da sala?
Etc_06_3	0,126	95,192	121,802	Manter a mesa limpa/organizada?
Etc_06_4	0,124	83,067	119,682	Proteger os documentos de trabalho de acesso não autorizado?
Gts_01_1	0,150	84,456	117,264	Avalia os riscos de danos ou incidentes como, perda, roubo, adulteração e acesso indevido aos dados.
Gts_01_2	0,142	80,903	112,257	Planeja a forma, o local, como os dados serão armazenados e acessados levando-se em consideração a avaliação dos riscos.
Gts_01_3	0,121	76,448	104,338	Leva em consideração as diretrizes estabelecidas pela sua organização no planejamento.
Gts_01_4	0,116	65,857	105,800	Executa os processos conforme planejado?
Gts_01_5	0,171	81,136	115,541	Avalia se os procedimentos adotados estão atendendo às necessidades de segurança.

Continuação				
item	a	b1	b2	Descrição do Item
Gts_01_6	0,092	67,813	115,806	Executa as modificações necessárias para adequar às novas necessidades?
Dmc_02_2	0,087	58,274	109,834	Estimula os colegas a emitirem opiniões, promove um ambiente participativo?
Rsc_01_1	0,093	92,153	131,563	Cópia de segurança em mídias externas. (CD, DVD, Storage, <i>Pendrive</i> ,...)
Rsc_01_3	0,118	95,644	130,070	Verifica se as cópias de segurança estão atualizadas.
Rsc_04_2	0,089	97,043	121,212	Passar o antivírus antes de abrir o anexo.
Rsc_04_3	0,079	54,890	88,239	Verificar a procedência do e-mail antes de abrir o anexo
Rsc_06_3	0,124	92,000	112,860	Passa o antivírus antes de abrir ou executar programas da mídia?
Rsc_11_3	0,077	56,337	102,712	Números, letra e caracteres especiais misturados.
Rsc_12_1	0,114	78,056	132,608	Trocar a sua senha de acesso?
Rsc_12_2	0,146	107,814	129,396	Criptografar os dados importantes?
Rsc_12_6	0,086	78,893	124,253	Limpar, higienizar o seu equipamento de trabalho?
Rsc_13_1	0,077	67,066	115,595	Verifica se o sítio é seguro?
Rsc_13_2	0,116	80,223	116,109	Verifica se a rede é segura?
Rsc_14_1	0,085	71,088	112,401	Verifica se alguém está te observando?
Rsc_14_2	0,115	95,996	119,812	Verifica se está sendo filmado?

Continuação				
item	a	b1	b2	Descrição do Item
Rsc_14_3	0,103	84,954	119,892	Verifica se o dispositivo que está utilizando está em bom estado de conservação?
Rsc_15_2	0,086	72,005	105,354	Procura saber a procedência do aplicativo?
Rsc_16_1	0,102	69,518	91,652	Confirma o conteúdo da mídia antes de descartar.
Rsc_16_2	0,077	66,890	102,789	Destrói ou encaminha a mídia para destruição.
Rsc_16_3	0,104	101,230	119,998	Registra o descarte ou a baixa da mídia.
Rsc_16_4	0,120	92,945	109,910	Verifica se a mídia está em conformidade com os requisitos para o seu descarte.
Prj_01_1	0,081	100,923		A política de segurança da Informação na sua organização está em que estágio?
Prj_02_1	0,135	96,100	113,772	Definição e elaboração do projeto.
Prj_02_2	0,236	86,206	112,267	Na execução do projeto.
Prj_02_3	0,206	83,123	112,541	No gerenciamento do projeto.
Rvl_01_1	0,171	92,500	125,016	Com que frequência você ou sua equipe revisa as políticas de segurança da informação da sua organização?
Rvl_01_2	0,116	110,130	132,235	Você é convidado(a) a participar da reavaliação das políticas de segurança da Informação.
Rvl_02_1	0,140	82,959	125,265	Com que frequência você reavalia as suas atitudes com respeito a segurança da informação?

Fonte: Próprio autor

APÊNDICE E – Frequência por escore

Tabela 14 - Frequência por escore

autoaval	Frequência escore (100,10)														Total
	65	70	75	80	85	90	95	100	105	110	115	120	125	130	
0	2	1	6	12	16	24	16	6	6	1	2	0	0	0	92
1	1	7	6	29	42	83	118	110	40	18	7	2	0	0	463
2	0	0	2	8	25	38	100	113	86	48	21	12	3	0	456
3	0	1	1	2	2	3	8	20	21	21	9	9	6	3	106
Total	3	9	15	51	85	148	242	249	153	88	39	23	9	3	1117

$$\chi^2 = 322,1$$

$$\text{g.l.} = 39$$

$$p < 2e^{-16}$$

APÊNDICE G – Quadro Comparativo de Metodologias de Maturidade

Quadro 9 - Análise Comparativa de Modelos de Maturidade da Segurança da Informação

Modelo de maturidade da segurança da informação	Orientação	Limitação e governança	Nível de maturidade					
			-3 a 0	1º	2º	3º	4º	5º
Ism3	Gestão de si avaliação de risco e integração de processos	Questões culturais organizacionais	-	Indefinido	Definido	Gerenciado	Controlado	Otimizado
Nist-prisma	Avaliação e documentação	Questões de segurança não técnicas	-	Políticas	Processo	Implementação	Teste	Implementando
Gsmm	Proteção de informações	Questões de segurança não técnicas	-	Confiando as cegas	Repetitivo	Definido	Gerenciado	Manutenção
Gismm	Sensibili-	Questões de	-	Blissfulig-	Consci-	Corretivo	Excelên-	

	zação para a segurança e gestão de riscos	segurança não técnicas		no rance	ênte		cia operacional	
Suny's isi	Proteção de segurança da informação	Questões de segurança não técnicas	-	Respon- dendo ao básico	Constru- indo proteção	Problemas de segurança	Manuten- ção da segurança	
Isf-ibm	Análise de falha de segurança	Questões de segurança não técnicas	-	Inicial	Basico	Capaz	Eficiente	Otimizado
Citi- isem	Sensibili- zação para a segurança e avalia- ção	Questões de segurança não técnicas	-	Compla- cente	Reco- nheci- mento	Integração	Praticas comuns	Melhoria contínua
Isms (im)	Controle de gestão	Garantia organizacio- nal e métri- cas	0:neglig ente 1:obstrut ivo 2:arrogan te 3:subver	Funcional	Técnico	Operacio- nal	Gerencia- do	Estratégico

			sivo					
Sse-cmm	Segurança do projeto de engenharia de	Orientação das melhor-práticas		Informalmente conduzido	Planejado e monitorados	Bem definido	Quantitativa-mente-controlado	Melhoria contínua
Cobit	Procedimentos de auditoria específicos	Processos de negócios	0. Não existe	Inicial/ad hoc	Repetitivo e intuitivo	Projetos definidos	Dirigido e mensurável	Otimizado

Fonte: (Karakola, Kowalski et al., 2011, p. 3; Stambul e Razali, 2011)