UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

Anna Cláudia dos Santos Nobre

FATORES QUE INFLUENCIAM A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO:

um estudo com gestores públicos estaduais no Brasil

NATAL-RN
2009

Livros Grátis

http://www.livrosgratis.com.br

Milhares de livros grátis para download.

Anna Cláudia dos Santos Nobre

FATORES QUE INFLUENCIAM A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO:

um estudo com gestores públicos estaduais no Brasil

Dissertação apresentada ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Norte como requisito para obtenção do título de Mestre em Administração.

Orientadora: Profª Dra. Anatália Saraiva Martins Ramos.

NATAL-RN
2009

Anna Cláudia dos Santos Nobre

FATORES QUE INFLUENCIAM A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO:

um estudo com gestores públicos estaduais no Brasil

Dissertação apresentada ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Norte como requisito para obtenção do título de Mestre em Administração.

Profª Dra. Anatália Saraiva Martins Ramos
Universidade Federal do Rio Grande do Norte - UFRN
Orientadora

Prof. Dr. Manoel Veras de Sousa Neto
Universidade Federal do Rio Grande do Norte - UFRN
Membro

Profª Dra. Maria Alexandra Viegas Cortez da Cunha
Pontifícia Universidade Católica do Paraná - PUC/PR
Membro

AGRADECIMENTOS

Em face da conclusão de mais uma etapa em minha vida, agradeço:

À Deus, por tudo;

Ao meu filho, João Felipe, fonte inesgotável de amor e inspiração;

Aos meus pais, João e Gentil, por serem sustentáculo moral de minha vida;

Às minhas irmãs, Katia e Carmen, pelo apoio e orações em todos os momentos de minha vida;

Ao meu irmão, Alexandre, à minha cunhada, Ligia, e aos meus sobrinhos, Beatriz e Marcus, pelo companheirismo;

Aos meus colegas da SEARH, em especial ao Secretário Paulo César, pelas oportunidades de crescimento profissional;

Aos meus colegas de setor de trabalho (UCE/PNAGE), em especial Thiago Limeira e Felipe Galvão, pela ajuda preciosa na tabulação dos dados e conferência desta pesquisa;

Aos meus colegas das unidades estaduais do PNAGE em todo o país, pelo apoio inestimável no preenchimento dos questionários;

Aos professores e funcionários do PPGA que tornaram possível a realização deste estudo, em especial à minha orientadora, Profa. Anatália, por seu exemplo de dedicação;

Aos meus colegas de turma do Mestrado, em especial Alixandre Santana e Bruno Campelo, pela ajuda em todos os momentos;

Enfim, agradeço a todos que direta ou indiretamente contribuíram para a concretização deste sonho, que me possibilitou adquirir novos conhecimentos e crescer como profissional, como pesquisadora e como pessoa.

"Não basta saber, é preciso também aplicar;
não basta querer, é preciso também fazer"

Johann Goethe

RESUMO

Este estudo analisa os fatores que influenciam os gestores públicos na adoção de práticas avançadas de Gestão de Segurança da Informação. A pesquisa utilizou como base assertivas da Norma de Segurança ISO 27001:2005 e modelo teórico baseado no TAM (*Technology Acceptance Model*) descrito em Venkatesh e Davis (2000). O método adotado foi a pesquisa de campo de alcance nacional que contou com a participação de oitenta gestores públicos dos Estados do Brasil, sendo todos coordenadores na área de gestão e planejamento dos governos estaduais. A abordagem da pesquisa foi quantitativa e foram utilizados métodos de estatística descritiva, análise fatorial e regressão linear múltipla para análise dos dados. Os resultados da pesquisa apresentaram correlação entre os construtos do modelo TAM (facilidade na utilização, percepção sobre a utilidade, atitude e intenção de utilização) e a concordância com as assertivas elaboradas de acordo com a norma ISO 27001, demonstrando que estes fatores influenciam os gestores na adoção de tais práticas. Já as outras variáveis independentes do modelo (perfil organizacional, perfil demográfico e comportamental dos gestores) não tiveram correlação significante com as assertivas da referida norma, demonstrando necessidade de ampliação de pesquisas com utilização de tais construtos. Espera-se que este estudo possa contribuir de forma positiva ao avanço nas discussões sobre o tema Gestão de Segurança da Informação e Adoção de Normas de Segurança, bem como, Modelos de Aceitação de Tecnologia.

Palavras-chave: Gestão de Segurança da Informação. Certificação ISO 27001. Modelo de Aceitação de Tecnologia TAM.

ABSTRACT

This study examines the factors that influence public managers in the adoption of advanced practices related to Information Security Management. This research used, as the basis of assertions, Security Standard ISO 27001:2005 and theoretical model based on TAM (Technology Acceptance Model) from Venkatesh and Davis (2000). The method adopted was field research of national scope with participation of eighty public administrators from states of Brazil, all of them managers and planners of state governments. The approach was quantitative and research methods were descriptive statistics, factor analysis and multiple linear regression for data analysis. The survey results showed correlation between the constructs of the TAM model (ease of use, perceptions of value, attitude and intention to use) and agreement with the assertions made in accordance with ISO 27001, showing that these factors influence the managers in adoption of such practices. On the other independent variables of the model (organizational profile, demographic profile and managers' behavior) no significant correlation was identified with the assertions of the same standard, witch means the need for expansion researches using such constructs. It is hoped that this study may contribute positively to the progress on discussions about Information Security Management, Adoption of Safety Standards and Technology Acceptance Model.

Keywords: Information Security Management. ISO 27001 Certification. Technology Acceptance Model TAM.

LISTA DE ILUSTRAÇÕES

Diagrama 1. Evolução da Conectividade e do Compartilhamento 29
Diagrama 2. Conceitos básicos e aspectos complementares de segurança da informação no ciclo de vida da informação. 32
Diagrama 3. Barreiras da Segurança. 37
Diagrama 4. Modelo de PDCA aplicado a processos de SGSI 48
Diagrama 5. TRA – Teoria da Ação Racional 53
Diagrama 6. Relação dos construtos do Modelo TAM 54
Diagrama 7. Modelo de Atitudes perante a tecnologia e informatização (MOATI) 56
Diagrama 8. Relação dos construtos do Modelo TAM2 57
Diagrama 9. Modelo teórico da pesquisa 68
Gráfico 1. Distribuição de frequências do tipo da organização 71
Gráfico 2. Distribuição de frequências do setor de atuação 71
Gráfico 3. Distribuição de frequência por região geográfica 72
Gráfico 4. Dispersão do Parque de Informática 72
Gráfico 5. Dispersão de Usuários da Rede 73
Gráfico 6. Distribuição de frequências de Incidência de ataque 74
Gráfico 7. Distribuição de frequências da Hierarquia do Setor de SI 75
Gráfico 8. Distribuição de frequências de área de atuação 75
Gráfico 9. Distribuição do sexo dosrespondentes 76
Gráfico 10. Distribuição de frequências do Nível de escolaridade 77
Gráfico 11 – Distribuição de frequências de Conhecimento geral em informática 77
Gráfico 12. Distribuição de frequências de Treinamento em rede e/ou segurança da informação 78
Gráfico 13. Distribuição de frequências do papel na adoção de novas tecnologias 78
Gráfico 14. Distribuição de frequências do uso de rede do trabalho para acessar contas pessoais 79
Gráfico 15. Distribuição de frequências das vezes que costuma fazer back up de seus arquivos 80
Gráfico 16. Respostas Modelo TAM - Facilidade de Utilização 1 80
Gráfico 17. Respostas Modelo TAM - Facilidade de Utilização 2 81

Gráfico 18. Respostas Modelo TAM – Percepções sobre a Utilidade 1 81
Gráfico 19. Respostas Modelo TAM – Percepções sobre a Utilidade 2 82
Gráfico 20. Respostas Modelo TAM – Atitude 1..... 82
Gráfico 21. Respostas Modelo TAM – Atitude 2..... 83
Gráfico 22. Respostas Modelo TAM – Intenção de Utilização 1..... 83
Gráfico 23. Respostas Modelo TAM – Intenção de Utilização 2..... 84
Diagrama 10. Modelo teórico da pesquisa revisto 136

LISTA DE TABELAS

Tabela 1. Quantitativo detalhado da população....61
Tabela 2. Distribuição e devolução dos questionários do PNAGE....63
Tabela 3. Distribuição e devolução dos questionários da ABEP....64
Tabela 4. Estatística descritiva do perfil organizacional....73
Tabela 5. Idade dos Respondentes....76
Tabela 6. KMO and Bartlett's Test....85
Tabela 7. Component Matrix....86
Tabela 8. Model Summary do Fator 1 (variável dependente) com Facilidade de Uso....90
Tabela 9. ANOVA do Fator 1 (variável dependente) com Facilidade de Uso....90
Tabela 10. Coefficients do Fator 1 (variável dependente) com Facilidade de Uso....90
Tabela 11. Model Summary do Fator 1 (variável dependente) com Utilidade Percebida....92
Tabela 12. ANOVA do Fator 1 (variável dependente) com Utilidade Percebida....92
Tabela 13. Coefficients do Fator 1 (variável dependente) com Utilidade Percebida....93
Tabela 14. Model Summary do Fator 1 (variável dependente) com Atitude....94
Tabela 15. ANOVA do Fator 1 (variável dependente) com Atitude....94
Tabela 16. Model Summary do Fator 1 (variável dependente) com Intenção de Uso....95
Tabela 17. ANOVA do Fator 1 (variável dependente) com Intenção de Uso....95
Tabela 18. Model Summary do Fator 1 (variável dependente) com Perfil Demográfico....96
Tabela 19 – ANOVA do Fator 1 (variável dependente) com Perfil Demográfico....96
Tabela 20. Model Summary do Fator 1 (variável dependente) com Perfil Comportamental....97
Tabela 21. ANOVA do Fator 1 (variável dependente) com Perfil Comportamental....97
Tabela 22. Model Summary do Fator 1 (variável dependente) com Perfil Organizacional....98
Tabela 23. ANOVA do Fator 1 (variável dependente) com Perfil Organizacional....98
Tabela 24. Model Summary do Fator 2 (variável dependente) com Facilidade de Uso....99
Tabela 25. ANOVA do Fator 2 (variável dependente) com Facilidade de Uso....99
Tabela 26. Model Summary do Fator 2 (variável dependente) com Utilidade Percebida....100
Tabela 27. ANOVA do Fator 2 (variável dependente) com Utilidade Percebida....100
Tabela 28. Model Summary do Fator 2 (variável dependente) com Atitude....101
Tabela 29. ANOVA do Fator 2 (variável dependente) com Atitude....101
Tabela 30. Model Summary do Fator 2 (variável dependente) com Intenção de Uso....101
Tabela 31. ANOVA do Fator 2 (variável dependente) com Intenção de Uso....102

Tabela 32. Model Summary do Fator 2 (variável dependente) com Perfil Demográfico 102
Tabela 33. ANOVA do Fator 2 (variável dependente) com Perfil Demográfico 102
Tabela 34. Model Summary do Fator 2 (variável dependente) com Perfil Comportamental 103
Tabela 35. ANOVA do Fator 2 (variável dependente) com Perfil Comportamental 103
Tabela 36. Model Summary do Fator 2 (variável dependente) com Perfil Organizacional ... 104
Tabela 37. ANOVA do Fator 2 (variável dependente) com Perfil Organizacional 104
Tabela 38. Model Summary do Fator 3 (variável dependente) com Facilidade de Uso 105
Tabela 39. ANOVA do Fator 3 (variável dependente) com Facilidade de Uso 105
Tabela 40. Model Summary do Fator 3 (variável dependente) com Utilidade Percebida..... 106
Tabela 41. ANOVA do Fator 3 (variável dependente) com Utilidade Percebida 106
Tabela 42. Model Summary do Fator 3 (variável dependente) com Atitude 107
Tabela 43. ANOVA do Fator 3 (variável dependente) com Atitude 107
Tabela 44. Model Summary do Fator 3 (variável dependente) com Intenção de Uso 107
Tabela 45. ANOVA do Fator 3 (variável dependente) com Intenção de Uso 108
Tabela 46. Coefficients do Fator 3 (variável dependente) com Intenção de Uso 108
Tabela 47. Model Summary do Fator 3 (variável dependente) com Perfil Demográfico 109
Tabela 48. ANOVA do Fator 3 (variável dependente) com Perfil Demográfico 109
Tabela 49. Model Summary do Fator 3 (variável dependente) com Perfil Comportamental 110
Tabela 50. ANOVA do Fator 3 (variável dependente) com Perfil Comportamental 110
Tabela 51. Model Summary do Fator 3 (variável dependente) com Perfil Organizacional ... 111
Tabela 52. ANOVA do Fator 3 (variável dependente) com Perfil Organizacional 111
Tabela 53. Model Summary do Fator 4 (variável dependente) com Facilidade de Uso 112
Tabela 54. ANOVA do Fator 4 (variável dependente) com Facilidade de Uso 112
Tabela 55. Model Summary do Fator 4 (variável dependente) com Utilidade Percebida..... 113
Tabela 56. ANOVA do Fator 4 (variável dependente) com Utilidade Percebida 113
Tabela 57. Coefficients do Fator 4 (variável dependente) com Utilidade Percebida 113
Tabela 58. Model Summary do Fator 4 (variável dependente) com Atitude 114
Tabela 59. ANOVA do Fator 4 (variável dependente) com Atitude 115
Tabela 60. Coefficients do Fator 4 (variável dependente) com Atitude 115
Tabela 61. Model Summary do Fator 4 (variável dependente) com Intenção de Uso 116
Tabela 62. ANOVA do Fator 4 (variável dependente) com Intenção de Uso 116
Tabela 63. Model Summary do Fator 4 (variável dependente) com Perfil Demográfico 117
Tabela 64. ANOVA do Fator 4 (variável dependente) com Perfil Demográfico 117
Tabela 65. Model Summary do Fator 4 (variável dependente) com Perfil Comportamental 118

Tabela 66. ANOVA do Fator 4 (variável dependente) com Perfil Comportamental 118
Tabela 67. Model Summary do Fator 4 (variável dependente) com Perfil Organizacional ... 119
Tabela 68. ANOVA do Fator 4 (variável dependente) com Perfil Organizacional 119
Tabela 69. Coefficients do Fator 4 (variável dependente) com Perfil Organizacional 119
Tabela 70. Model Summary do Fator 5 (variável dependente) com Facilidade de Uso 121
Tabela 71. ANOVA do Fator 5 (variável dependente) com Facilidade de Uso 121
Tabela 72. Coefficients do Fator 5 (variável dependente) com Facilidade de Uso 121
Tabela 73. Model Summary do Fator 5 (variável dependente) com Utilidade Percebida 122
Tabela 74. ANOVA do Fator 5 (variável dependente) com Utilidade Percebida 122
Tabela 75. Model Summary do Fator 5 (variável dependente) com Atitude 123
Tabela 76. ANOVA do Fator 5 (variável dependente) com Atitude 123
Tabela 77. Coefficients do Fator 5 (variável dependente) com Atitude 124
Tabela 78. Model Summary do Fator 5 (variável dependente) com Intenção de Uso 125
Tabela 79. ANOVA do Fator 5 (variável dependente) com Intenção de Uso 125
Tabela 80. Coefficients do Fator 5 (variável dependente) com Intenção de Uso 125
Tabela 81. Model Summary do Fator 5 (variável dependente) com Perfil Demográfico 127
Tabela 82. ANOVA do Fator 5 (variável dependente) com Perfil Demográfico 127
Tabela 83. Model Summary do Fator 5 (variável dependente) com Perfil Comportamental 128
Tabela 84. ANOVA do Fator 5 (variável dependente) com Perfil Comportamental 128
Tabela 85. Model Summary do Fator 5 (variável dependente) com Perfil Organizacional ... 128
Tabela 86. ANOVA do Fator 5 (variável dependente) com Perfil Organizacional 129

SIGLAS

ABEP	Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação
ABNT	Associação Brasileira de Normas Técnicas
BSC	Balanced Scoredcard
BID	Banco Interamericano de Desenvolvimento
CobiT	Control Objectives for Information and related Technology
CTCPEC	Produtos Confiáveis para Computadores do Canadá
DoD	Departamento de Defesa dos Estados Unidos da América
DTI	Departamento de Comércio e Indústria Britânico
EAL	Nível de Avaliação de Segurança
FC	Critério federal dos Estados Unidos
GCHQ	Quartel general de Comunicações do Governo Britânico
IEC	Consórcio de Engenharia Internacional
ISO	Organização Internacional para Normalização
ISS	Sucesso do Sistema de Informação
ITIL	Information Technology Infrastructure Library
ITSEC	Critério de Avaliação de Segurança da Tecnologia da Informação Confiável
MOATI	Modelo Organizacional de Atitudes perante a Tecnologia da Informação
NIST	Instituto Nacional de Padrões e Tecnologia dos Estados Unidos da América
NVLAP	Programa de Normas Nacional dos Estados Unidos da América
OCDE	Organização para a Cooperação e o Desenvolvimento Econômico
PNAGE	Programa Nacional de Apoio a Modernização da Gestão e do Planejamento dos Estados e do Distrito Federal
PP	Perfil de Proteção
PPGA	Programa de Pós-Graduação em Administração
SAR	Requerimentos de Garantia de Segurança
SCC	Conselho de Normas do Canadá
SFR	Requisito de Segurança Funcional
SGSI	Sistema de Gestão de Segurança da Informação
ST	Objetivo da Segurança

TAM	Modelo de Aceitação de Tecnologias
TCB	Base de Computação Confiável
TCSEC	Critério de Avaliação de Segurança da Informação Confiável
TI	Tecnologia da Informação
TIC	Tecnologia da informação e Comunicação
TOE	Alvo da Avaliação
TPB	Teoria do Comportamento Planejado
TRA	Teoria de Ação Racional
TRI	Índice de prontidão para o uso de tecnologia
TTF	Ajuste da Tarefa Computacional
UCE	Unidade de Coordenação Estadual
UFRN	Universidade Federal do Rio Grande do Norte
UKAS	Serviço de Normas do Reino Unido

LISTA DE QUADROS

Quadro 1. Trabalhos correlatos em segurança da informação..... 24
Quadro 2. Conceitos importantes em segurança da informação..... 33
Quadro 3. Níveis de segurança conforme TCSEC..... 42
Quadro 4. Conceitos do common criteria..... 44
Quadro 5. Normas operacionais da série 27001..... 46
Quadro 6. Domínios da norma ISO 27001..... 49
Quadro 7. Trabalhos correlatos em modelos de aceitação de tecnologias..... 52
Quadro 8. Definição dos construtos do modelo TAM 3..... 59
Quadro 9. Correspondência entre modelo, hipóteses e questionário..... 69
Quadro 10. Fatores da pesquisa..... 87
Quadro 11. Validação das hipóteses..... 129

SUMÁRIO

1. INTRODUÇÃO 17
1.1 CONTEXTUALIZAÇÃO 17
1.2 PROBLEMATIZAÇÃO 18
1.3 OBJETIVOS 20
1.3.1 Geral 20
1.3.2 Específicos 21
1.4 JUSTIFICATIVA 21
1.5 ESTRUTURA DO TRABALHO 23
2. REFERENCIAL TEÓRICO 24
2.1 SEGURANÇA DA INFORMAÇÃO 24
2.1.1 Evolução da Tecnologia e da Segurança da Informação 25
2.1.2 Conceitos relacionados com a Segurança da Informação 31
2.1.3 Segurança da Informação no Setor Público 39
2.2 MODELOS DE CERTIFICAÇÃO EM SEGURANÇA DA INFORMAÇÃO 41
2.2.1 Norma ISO/IEC 27001 45
2.3 MODELOS DE ACEITAÇÃO DE TECNOLOGIA 50
3. METODOLOGIA 60
3.1CLASSIFICAÇÕES METODOLÓGICA DA PESQUISA 60
3.2 POPULAÇÃO E AMOSTRA DA PESQUISA 60
3.3 MÉTODO DA PESQUISA E INSTRUMENTO DA COLETA DE DADOS 62
3.4 OPERACIONALIZAÇÃO DAS VARIÁVEIS 65
3.5 MODELO DA PESQUISA 67
4. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS 70
4.1 ESTATÍSTICA DESCRITIVA 70
4.2 ANÁLISE FATORIAL 84
4.3 ANÁLISE DE REGRESSÃO MÚLTIPLA 88
4.3.1 Análise de Regressão Múltipla para o Fator 1-Usuários 90
4.3.2 Análise de Regressão Múltipla para o Fator 2-Senhas 98
4.3.3 Análise de Regressão Múltipla para o Fator 3-Biometria 104
4.3.4 Análise de Regressão Múltipla para o Fator 4-Férias 111
4.3.5 Análise de Regressão Múltipla para o Fator 5-Desligamento 120

4.4 VALIDAÇÃO DAS HIPÓTESES PROPOSTAS 129
5. CONSIDERAÇÕES FINAIS 135
REFERÊNCIAS 138
APÊNDICES 147

1. INTRODUÇÃO

Esta seção é composta pela contextualização no tema, revisando fatos históricos que evoluíram para a problematização, também apresentada nesta parte do estudo. Os objetivos também são listados, bem como as justificativas do ponto de vista teórico, prático, social e pessoal. Este capítulo encerra com uma subseção explicativa da estrutura do trabalho.

1.1 CONTEXTUALIZAÇÃO

As tecnologias tiveram destaque na Revolução Industrial como uma forma de agilizar os processos operacionais. No entanto, com o passar dos anos, elas vêm assumindo os papéis mais diversos dentro das organizações na busca por formas mais rápidas, fáceis, eficientes e competitivas de realizar trabalhos distintos.

Castells (1999) detalha em seus estudos que houve pelo menos duas Revoluções Industriais: a do final do século XVIII com as máquinas a vapor e os avanços da metalurgia; e cem anos depois com a eletricidade e todos os equipamentos criados advindos desta. Seguindo os passos de tais avanços mecanográficos e com base em uma vasta quantidade de descobertas, ocorre a Revolução da Tecnologia da Informação que teve como marco importante a década de 70 com a invenção do microprocessador e do microcomputador.

Com o passar dos anos, a Tecnologia da Informação (TI) assumiu uma diversificação de funções dentro das organizações e sua importância passou a se relacionar com seu nível estratégico, ou seja, ela deixou de exercer um papel meramente operacional e passou a ser ferramenta essencial no apoio a tomada de decisão. Castells (1999) destaca que a Revolução da TI foi responsável por uma série de alterações sociais, inclusive em relação a empregos e avanço comercial dos países mais evoluídos nesta área.

Com recentes descobertas tecnológicas e os efeitos da globalização, mais um conceito foi agregado a esta área, hoje é muito mais comum falar-se em Tecnologia da

Informação e Comunicação (TIC), pois a comunicação passou a ser uma forma indispensável na utilização da informação. Desta forma a TIC assumiu, no decorrer dos últimos anos, funções inerentes ao controle gerencial da empresa que podem diferenciá-la da concorrência. Como forma de facilitar a compreensão e pelo fato da comunicação estar intrinsecamente relacionada às funções da tecnologia atual, assume-se neste texto que o termo TI também incorpora o conceito de comunicação.

Oliveira (1994) alega que o crescimento de informações, as novas tecnologias de comunicação e de banco de dados são fortes impulsionadores da atual transformação da sociedade. Assim, a informação passou a ser considerada um dos bens mais valiosos dentro de qualquer organização e manter este bem seguro, confiável e acessível a todos os que têm direito a conhecê-lo passou a ser um fator fundamental e diferencial que poderá possibilitar sua sobrevivência no mercado.

Baldissera e Nunes (2007) corroboram tal pensamento quando defendem que por vivermos em um momento onde a informação é fundamental para qualquer tipo de organização, a adequada Gestão da Segurança da Informação é uma necessidade inevitável. Tais autores defendem que gerir significa adotar normas.

Asciutti (2006) também defende que a informação é um ativo de valor nas organizações e sua proteção de ataques externos e internos é o objetivo da segurança computacional. O autor apresenta um modelo de política de segurança baseado na Norma ABNT ISO.

A ABNT (Associação Brasileira de Normas Técnicas) em conjunto com a Organização Internacional para Normalização (*International Organization for Standartization – ISO*) elaborou a versão brasileira da norma ISO 27001, que promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o Sistema de Gerenciamento da Segurança da Informação - SGSI de uma organização.

1.2 PROBLEMATIZAÇÃO

Diante de um contexto de crescimento da importância da área de TI dentro das organizações também cresceu a importância de manter esta estrutura segura. Campos (2006)

destaca que a informação é um elemento essencial para as organizações que, por estar permeada em todas as áreas da organização, em diversas formas, e por ter se transformado num ativo importante, precisa ser protegido. A segurança dos dados de uma empresa inclui desde a preservação da integridade dos equipamentos até as informações que estão armazenadas neles.

Falhas nesta estrutura podem resultar em quebras da confidencialidade, através de acesso por pessoas não autorizadas; da integridade, através de alteração indevida de dados; e da disponibilidade, com a acessibilidade não permitida a quem é autorizado (SÊMOLA; 2003). Fatores como a alta conectividade, através da utilização de redes de computadores e a própria internet, aumentaram nas empresas tanto a vulnerabilidade quanto a preocupação com tais falhas.

Quando se pesquisa estudos acadêmicos na área de Segurança da Informação, é mais frequente a existência de pesquisas de cunho técnico que gerencial. Mesmo os gerenciais, são focados em casos específicos, telecomunicações ou estratégicas empresariais que levam pouco em consideração a aceitação na adoção por parte dos usuários (CARVALHO, 2003; FONSECA, 2003; LESSA, 2004; CURTI, 2004; MENEZES, 2005; LIMA, 2006; BAUER, 2006; ASSMANN, 2006; SILVA NETTO, 2007; RAMOS, 2007; SOUZA, 2007; LORENS, 2007; FRÓIO, 2008; SILVA, 2008).

Mas, o que leva um usuário a adotar certos recursos tecnológicos? Muitas pesquisas são realizadas para analisar a aceitação de usuários na adoção de tecnologias. Para tanto, existem diversos modelos de verificação de aceitação de tecnologia e um dos mais conhecidos é o modelo TAM – *Technology Acceptance Model*.

Tanto o modelo TAM quanto suas adaptações e as teorias que lhe deram origem foram testadas em vários tipos de organizações e para as mais diversas áreas, como ERP, EAD, Compras Eletrônicas, dentre outras (VENKATESH; DAVIS, 1996; MORRIS; VENKATESH, 2000; VENKATESH; 2000; DIAS; ZWICKER; VICENTIN, 2003; BUENO; ZWICKER; OLIVEIRA, 2004; COSTA FILHO; PIRES, 2004; OLIVEIRA; JOIA, 2004; SANTOS; AMARAL, 2004; ALMEIDA; SOBRAL, 2005; CARVALHO; FERREIRA, 2005; COSTA FILHO; PIRES, 2005; BROWN; VENKATESH; BALA, 2005; LÖBLER; VISENTINI; VIEIRA, 2006; RODRIGUES; COSTA, 2006; PIRES; YAMAMOTO; COSTA FILHO, 2006; SILVA; DIAS, 2006; OLIVEIRA JUNIOR, 2007; OLIVEIRA; RAMOS, 2008; SILVA; DIAS; SENA JUNIOR, 2008; SILVA, 2009), no entanto, existem poucos estudos utilizando o referido modelo ou suas adaptações para a área de Gestão de Segurança

da Informação, e os encontrados não se utilizam da norma mais recente da ISO na área, a ISO 27001:2005 (CAVALCANTE, 2003; GABBAY, 2003).

Os estudos pesquisados também ressaltam uma falta de estudos específicos para governos, o que se torna preocupante, tendo em vista as especificidades legais e culturais que diferem o setor público do privado. Em organizações públicas, problemas relacionados à segurança de dados tomam proporções maiores por afetarem um número maior de pessoas, já que todos os cidadãos devem ter acesso e se utilizar dos serviços ofertados pelos órgãos de governo. Outra preocupação específica da área pública é a viabilidade de uma estrutura segura, mas ágil e que não sofra descontinuidade pelas dificuldades de contratação impostas pela legislação.

Diante da problemática exposta, verifica-se a importância de estudos que relacionem os Gestores Públicos com as práticas de Gestão de Segurança da Informação, uma vez que a adoção de práticas nas organizações públicas depende fortemente do apoio ou decisão de tais gestores. Assim, esta pesquisa busca responder a seguinte questão:

Que fatores influenciam gestores públicos estaduais nas suas percepções em relação à aceitação de práticas avançadas de Gestão da Segurança da Informação?

1.3 OBJETIVOS

1.3.1 Geral

Analisar os fatores que influenciam gestores públicos estaduais nas suas percepções em relação à aceitação de práticas avançadas de Gestão da Segurança da Informação.

1.3.2 Específicos

- Descrever o padrão organizacional de uso da TI;
- Descrever o perfil demográfico dos gestores públicos;
- Descrever o perfil comportamental dos gestores públicos;
- Aferir a percepção de aceitação dos gestores públicos quanto às práticas avançadas em Gestão de Segurança da Informação, em conformidade com as diretrizes da Norma ISO 27001;
- Verificar as relações existentes entre o perfil dos gestores públicos, perfil organizacional e a aceitação de Normas Avançadas de Gestão de Segurança da Informação.

1.4 JUSTIFICATIVA

O Governo Federal Brasileiro iniciou em 2003 ações do Programa Nacional de Apoio a Modernização da Gestão e do Planejamento dos Estados e do Distrito Federal (PNAGE). O Ministério do Planejamento, Orçamento e Gestão, juntamente com o Banco Interamericano de Desenvolvimento (BID) e as Secretarias de Gestão e de Planejamento das Unidades da Federação Estaduais e o Distrito Federal, realizou diagnóstico que compreendeu dentre outras, a área de Sistemas de Informação (MPOG-BRASIL; 2008). Tal diagnóstico foi composto por questionários e entrevistas realizadas com gestores em cada uma das unidades da federação pesquisadas. Em sua avaliação conclusiva, foi detectada como uma das áreas mais preocupantes nos governos estaduais a Tecnologia da Informação.

Após a conclusão do diagnóstico, foi feito o marco lógico do programa composto por áreas e ações de solução para os problemas que poderiam ser incorporadas aos projetos específicos de cada Estado e do Distrito Federal. Em diversas Unidades da Federação um dos problemas mais ressaltados pelo diagnóstico foi a “descordenação das ações de TI”, que teve como uma das soluções sugeridas pelos gestores entrevistados a criação e implementação de Política de Segurança de Informações e Sistemas.

A avaliação feita pelo diagnóstico do PNAGE destaca que a área de Segurança da Informação é crítica para os Governos Estaduais e que ela merece atenção especial dos gestores. Outro fator que justifica a importância deste trabalho é que o setor público tem obrigações constitucionais de preservar a igualdade, transparência e democracia e estes fatores podem ser severamente ameaçados por falhas na segurança dos dados e informações governamentais.

Assim, a importância de um trabalho sobre Gerenciamento de Segurança da Informação na área pública não se resume a questões financeiras, mas também é uma forma de garantir que os direitos dos cidadãos sejam preservados e que as instituições governamentais não fracassem na realização de suas funções mais básicas.

A **relevância científica** do trabalho ocorre por ser uma oportunidade de avanço de conhecimento numa área de escassez de estudos, já que a maioria dos trabalhos de Segurança da Informação trata prioritariamente de questões técnicas (não gerenciais), conforme artigos pesquisados. Outro fator proeminente é a especificidade do foco no setor público, o que o torna ainda mais raro, portanto o trabalho pretende disponibilizar novos conhecimentos na área de Gestão de Segurança da Informações, baseados na Norma ISO/IEC 27001, preenchendo uma lacuna teórica e científica no tema estudado. Além disso, são apresentados modelos de pesquisa que podem ser utilizados em trabalhos futuros.

Em suma, do ponto de vista **teórico**, o trabalho justifica-se pela escassez de estudos de Gestão de Segurança da Informação; escassez de estudos sobre o tema específicos para área pública; escassez de estudos sobre a Norma ISO/IEC 27001 de 2005; necessidade de avanço do conhecimento de segurança da informação com enfoque em gestão pública; além de vinculação à linha de pesquisa existente no PPGA (Programa de Pós-Graduação em Administração) da UFRN de Gestão de Tecnologia da Informação, onde a pesquisa foi conduzida.

A **relevância prática** é outro aspecto a ser considerado, pois os resultados da pesquisa podem contribuir como base para elaboração de guias de orientação de investimento na Segurança de Informação para gestores públicos e como modelo de diagnóstico de segurança em organizações públicas.

Do ponto de vista **pessoal**, o trabalho justifica-se pelo fato da pesquisadora ter realizado anteriormente trabalho sobre terceirização, onde o tema Gestão de Segurança da Informação no setor público despontou como relevante pela preocupação demonstrada pelos gestores públicos entrevistados. Já do ponto de vista **social**, a pesquisa pode contribuir para organizações públicas através do fornecimento de subsídios a trabalhos técnicos de melhoria

na área; e possibilidade de evitar perdas de dados e ações preventivas ou até mesmo para aferir se as ações já implementadas estão em sintonia com o nível de concordância dos gestores, resultando assim em maior economia e eficiência.

1.5 ESTRUTURA DO TRABALHO

Este trabalho é composto de cinco capítulos, conforme a seguir.

O **primeiro capítulo** destaca na parte introdutória uma breve contextualização com a descrição da evolução da TI e da Segurança da Informação; a problematização, onde se explica como surgiu o problema da pesquisa; os objetivos gerais e específicos; e as justificativas deste trabalho, caracterizando-o como cientificamente relevante.

O **segundo capítulo** contém a fundamentação teórica através de subseções que destacam a Evolução e Conceitos importantes sobre Segurança da Informação, os Modelos de Certificação em Segurança da Informação e os Modelos de Aceitação de Tecnologia.

O **terceiro capítulo** detalha os aspectos metodológicos da pesquisa, através de uma breve descrição da Classificação Metodológica; População e Amostra da Pesquisa; Métodos e Técnicas que utilizados; Instrumento de Coleta; Operacionalização das Variáveis; Modelo Teórico utilizado.

O **quarto capítulo** que contém a apresentação e discussão dos resultados da pesquisa, detalhando os tipos de análise estatística adotados e os resultados obtidos, inclusive em relação às Hipóteses.

O trabalho é finalizado no **quinto capítulo** com a conclusão da pesquisa com suas considerações finais, detalhamento de limitações e propostas para estudos futuros.

Na parte final do trabalho constam as referências e apêndices com instrumentos de coleta de dados, controle de entrega dos questionários e tabelas.

2. REFERENCIAL TEÓRICO

Esta parte da pesquisa contém a fundamentação teórica dos três pilares do trabalho, a saber: Segurança da Informação; Modelos de Certificação de Segurança da Informação, com enfoque maior no modelo adotado neste estudo (ISO 27001) e; Modelos de Aceitação de Tecnologia, aprofundando no modelo utilizado com base desta pesquisa (TAM).

2.1 SEGURANÇA DA INFORMAÇÃO

Na área de Segurança da Informação, é mais comum encontrar pesquisas com enfoque técnico que gerencial e ainda a escassez é ampliada para o setor público, conforme demonstrado no quadro 1.

Ano	Autor(es)	Área de Pesquisa/Foco
2003	CARVALHO	Setor de Telecomunicações
	FONSECA	Estudo de Caso da Petrobras
2004	LESSA	Revisão de Literatura – Alinhamento Estratégico
	CURTI	Plataformas Unix e Windows
2005	MENEZES	Estudo de Caso em três organizações
2006	LIMA	Estudo de Caso Inmetro – Liderança
	BAUER	Redes Corporativas
	ASSMANN	Teoria da Complexidade
2007	SILVA NETTO	Pequenas e Médias Empresas
	RAMOS	Ciência da Informação
	SOUZA	Ferramentas e técnicas ISO 27001 e 17799
	LORENS	Cadeia de Regulamentação
2008	FRÓIO	Revisão de Literatura – Modelo Faseado
	SILVA	Modelo Funcional e de Competências

Quadro 1. Trabalhos correlatos em segurança da informação
Fonte: Próprio autor (2009)

Esta seção apresenta referencial teórico do tema Segurança da Informação e ela foi dividida em três subseções, a primeira onde é relatada a evolução da importância da informação e sua segurança das organizações, a segunda trata de conceitos importantes na

área de segurança da informação e a última descreve algumas peculiaridades de Gestão de Segurança da Informação para o setor público.

2.1.1 Evolução da Tecnologia e da Segurança da Informação

Castells (1999) informa que os pesquisadores apontam pelo menos dois períodos importantes cujas descobertas são consideradas como Revolução Industrial, sendo o primeiro deles as descobertas nas áreas de máquinas a vapor e metalurgia, no final do século XVIII, e o segundo, cem anos após o primeiro, onde houve avanços nas áreas da eletricidade e comunicação.

Em tal período, as tecnologias eram utilizadas como uma forma de tornar os processos operacionais das indústrias mais ágeis; no entanto, com o passar dos anos, ela vem assumindo os papéis mais diversos dentro das organizações na busca por formas mais rápidas, fáceis, eficientes e competitivas de realizar trabalhos distintos. Castells (1999) esclarece sobre a Revolução da Tecnologia da Informação na qual o foco é retirado do **pós-industrialismo** e, passa para o **informacionismo**, onde a maximização da produção é fundamentada no conhecimento por intermédio dos avanços tecnológicos.

As descobertas tecnológicas da década de 70, como o microprocessador e o microcomputador possibilitaram avanços significativos. Atualmente, a informação é considerada um ativo importante e, o setor que a gere tornou-se ponto estratégico nas organizações (CASTELLS, 1999; MOREIRA, 2001; SÊMOLA, 2003; VASCONCELOS, RICCIO; 2004; VIEIRA, 2004; CAMPOS, 2006; LUCAS JUNIOR, 2006). Joia (2004) reforça tais afirmações quando defende que, já no início da década de 80, a Tecnologias da Informação (TI) não era mais utilizada apenas como uma ferramenta de processamento mais rápido e sim como uma arma estratégica.

Na área da Gestão Pública, Barnum (2002) destaca que as ferramentas da Tecnologia da Informação exercem um papel de destaque na acessibilidade da informação ao cidadão. No Brasil, existem casos com ampla divulgação da utilização de tecnologias como mecanismos de cidadania, como é o caso das urnas eletrônicas e das centrais de atendimento online, sendo que, no primeiro, o exercício do voto e sua apuração tornaram-se mais ágeis e

no segundo foi facilitada a utilização de diversos serviços através de sistemas informatizados de muitos setores do governo em um único ambiente.

Oliveira (1994) alega que o crescimento de informações, as novas tecnologias de comunicação e de banco de dados são fortes impulsionadores da atual transformação da sociedade. O resumo do Simpósio realizado pela Organização para a Cooperação e o Desenvolvimento Econômico ocorrido em Barcelona sobre "*O Governo do Futuro*" corrobora esta informação, acrescentando que os avanços tecnológicos estão mudando a economia e, consequentemente, produzindo mudanças sociais (OCDE; 2001). Segundo tal resumo, estas mudanças ocorrem pela possibilidade de melhorar os serviços, prestar serviços mais rápidos, realizar um maior número de serviços e aumentar a democracia. O simpósio concluiu que a utilização de tecnologia permite o restabelecimento da confiança dos cidadãos com os governos, ampliando desta forma o destaque desta área para os gestores públicos.

Ruediger (2002) enfoca a oportunidade de a TI ser utilizada como ferramenta para constituir um "*Estado Virtual*" promotor de mudanças institucionais, transparência de governo e reinvenção do próprio governo real. Isso pela articulação em rede dos diversos segmentos da administração, pela transparência de processos e sua maior eficiência. O autor, no entanto, destaca a preocupação com a chamada exclusão digital, que é a dificuldade de acesso aos serviços públicos para as pessoas com dificuldades de compreensão das novas tecnologias, seja por falta de oportunidade ou por falta de interesse; os que se autoexcluem. Akutsu e Pinho (2002) e Cunha *et al.* (2005) propõem o termo democracia eletrônica ou *e-democracia*, sustentando que tal situação pressupõe o uso intensivo de ferramentas de TIC para possibilitar o contato entre o cidadão e o governo. A partir do emprego dessas ferramentas tecnológicas, os autores entendem que todos os sujeitos que fazem parte ou que deveriam fazer parte dos processos democráticos, podem efetivamente inserir-se nesse contexto.

Outros autores destacam o conceito de exclusão digital como um fator complicador na utilização de tecnologias para serviços públicos sem antes realizar uma equiparação de acessos para que todos os cidadãos tenham igualdade de direito (MACADAR; REINHARD, 2002; OLIVEIRA; CUNHA; SANTOS FILHO, 2003). Apesar das dificuldades oriundas da utilização de tecnologias para promover serviços públicos utilizando TI, Gore (1998) defende a criação de uma cidade eletrônica mundial para possibilitar acesso dos cidadãos a todos os serviços do governo de forma universal e globalizada, enquanto Moon (2002) destaca que a TI tem se tornado um dos elementos mais importantes da governança no futuro, considerando governança como capacidade do governo exercer suas funções. O autor

ainda cita que a TI está contribuindo para mudanças políticas, gerenciamento de performances de governo e redução da papelada.

Holden (1999) apud Oliveira, Cunha e Santos Filho (2003) descreve a evolução da administração da TI no setor público, em três estágios: 1) Administração de Sistemas de Informações; 2) Administração dos Recursos de Informação e 3) Administração de Tecnologia da Informação na Era da Informação. A evolução administrativa de TI no setor público diante de tais estágios alinha-se aos conceitos de maximizar a eficiência e reduzir os gastos. Com isso, o autor promove uma discussão sobre o avanço da importância da informação nas organizações.

Apesar de suas vantagens tão divulgadas, a TI não pode ser vista como a solução de todos os problemas. Vaz (2002) alerta sobre a importância de que os gestores públicos encarem a Tecnologia da Informação como ferramenta importante e potente, mas não como solução mágica. Segundo ele a tecnologia não pode ser vista como objetivo em si, mas como meio.

Diante do crescimento da importância da Gestão da Informação dentro das organizações, iniciaram-se as discussões acerca da importância de se definir papéis e estratégias na condução do ativo **informação**. A chamada Governança de TI é um conceito emergente e que serve como forma de conferir solidez e confiabilidade ao setor que gere a TI nas organizações (VASCONCELOS; RICCIO, 2004). É a combinação de estruturas e processos adotados por uma organização para garantir que os investimentos em tecnologia estejam alinhados com os objetivos de negócio, minimizar os riscos associados aos ativos informacionais, e otimizar a alocação dos recursos de TI. Existem modelos de processos baseados em melhores práticas que são rotulados como Governança de TI, dentre eles: o *Balanced Scoredcard* (BSC), o *Control Objectives for Information and related Technology* (CobiT) e o *Information Technology Infrastructure Library* (ITIL).

O **BSC** é uma metodologia desenvolvida em 1992 por Robert Kaplan e David Norton, professores da *Harvard Business School*. Os passos da implementação desta metodologia utiliza indicadores de desempenho para: i) definição da estratégia empresarial; ii) gerência do negócio; iii) gerência de serviços; e iv) gestão da qualidade. Os requisitos para definição de tais indicadores tratam dos processos de um modelo da administração de serviços e busca da maximização dos resultados baseados em quatro perspectivas que refletem a visão e estratégia empresarial: i) financeira; ii) clientes; iii) processos internos; iv) aprendizado e crescimento (BALANCED SCOREDCARD INSTITUTE; 2009).

O **CobiT** é um guia de boas práticas apresentado como *framework* criado e mantido pelo ISACA (*Information Systems Audit and Control Association*). Ele possui recursos que podem servir como um modelo de referência para gestão da TI, incluindo um sumário executivo, um *framework*, controle de objetivos, mapas de auditoria, ferramentas para a sua implementação e um guia com técnicas de gerenciamento. Este modelo pode ser utilizado como ferramenta para aumentar o retorno sobre o investimento (ROI) percebido, fornecendo métricas para avaliação dos resultados. Ele cobre quatro domínios, que possuem quatro processos, a saber: i) planejar e organizar; ii) adquirir e implementar; iii) entregar e dar suporte; iv) monitorar e avaliar (ISACA; 2009).

ITIL é um conjunto de boas práticas a serem aplicadas na infraestrutura, operação e manutenção de serviços de TI. Foi desenvolvido no final dos anos 80 pela CCTA (*Central Computer and Telecommunications Agency*) e atualmente está sob custódia da OGC (*Office for Government Commerce*) da Inglaterra. Este modelo busca promover a gestão com foco no cliente e na qualidade dos serviços TI (ITIL; 2009).

Mendonça (2007) apresenta cinco fatores motivadores da Governança de Tecnologia da Informação, a saber: o ambiente do negócio, os marcos de regulação, a integração tecnológica, os negócios de TI e a Segurança da Informação. Acerca da Segurança da Informação, alerta que a complexidade em sua gestão ficou mais complexa com a internet, ampliando riscos aos ativos organizacionais. Como se pode verificar a Governança de TI engloba diversas áreas de estudo em relação à Tecnologia da Informação, como: desenvolvimento de sistemas, gestão de *datacenter*, terceirização, riscos, alinhamentos estratégico da TI, gestão da qualidade, auditoria e Gestão de Segurança da Informação.

Tendo assumido o papel estratégico, a informação passou a ser visada como algo extremamente valoroso e, com isso, qualquer falha no acesso a esta informação passou a ser causa de prejuízo e até ruína de algumas empresas. Informações que chegam primeiramente na concorrência ou que são adulteradas de forma criminosa são motivo de preocupação para os gestores organizacionais.

A situação foi agravada com a evolução tecnológica nas telecomunicações. A internet que foi estabelecida como uma forma de atender pesquisas militares norte-americanas expandiu-se na década de 90 com a criação da *World Wide Web*, denominada web (BERNERS-LEE; 2009). Lucas (2006) defende que a próxima contribuição da tecnologia é sua habilidade de apoiar a comunicação e colaboração. Este novo ambiente foi percebido pelas organizações como uma possibilidade de expansão de negócios e consequente ampliação de lucros no ambiente privado.

A informação que era mantida anteriormente em grandes computadores de processamento centralizado, os *mainframes*, passou a trafegar pelas Redes de Computadores, em seguida pela internet e, atualmente, se utilizam os meios mais diversos para envio de informações, notebooks, celulares e muitos outros dispositivos de comunicação (SÊMOLA; 2003). Tal aspecto expansivo que pode ser visto como um avanço pela ampliação da velocidade e melhoria do acesso também resulta em dificuldades de gerenciamento da segurança. O diagrama 1 mostra a evolução da conectividade e do compartilhamento.

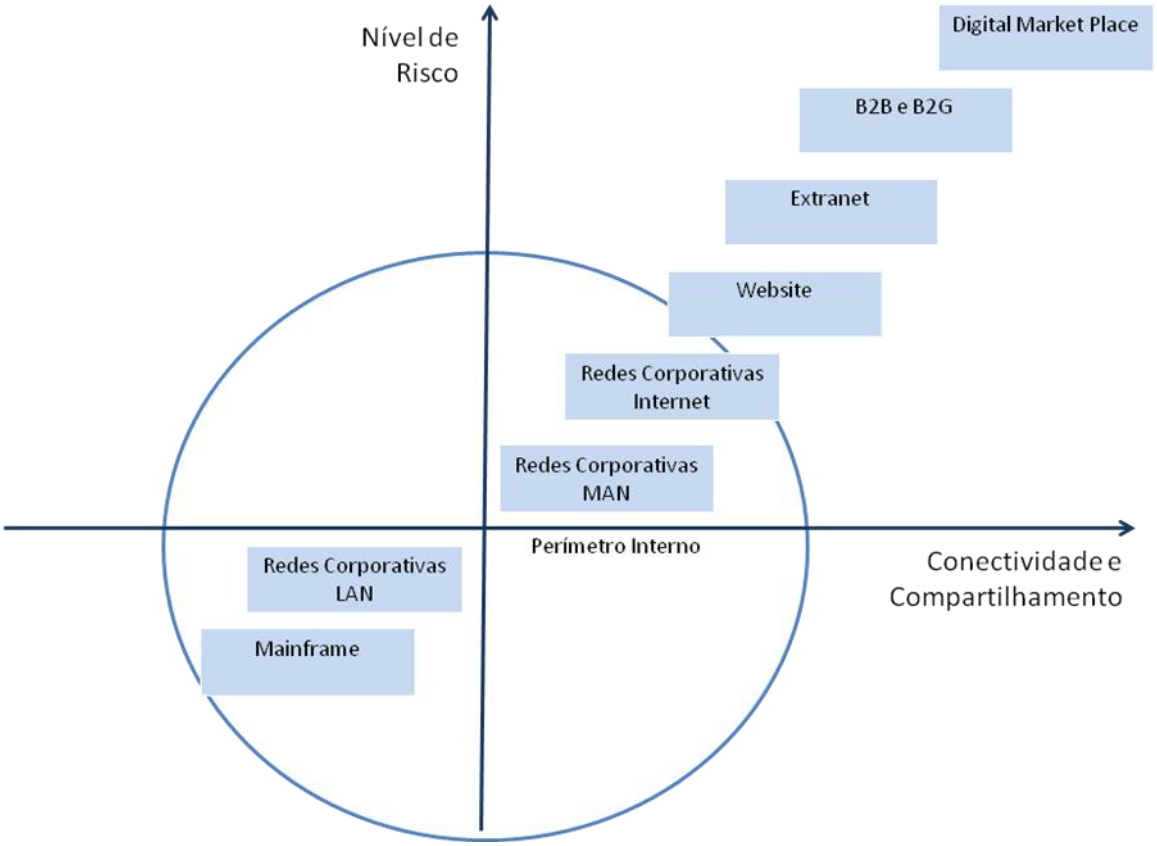


Diagrama 1. Evolução da conectividade e do compartilhamento
Fonte: Sêmola (2003)

Do diagrama 1 pode se extrair o crescimento das dependências das organizações em relação à informação e conectividade. Décadas atrás, a tecnologia tinha uso mais restritivo pelas limitações de armazenamento e preços proibitivos dos *mainframes*. Pouco tempo depois, compartilhar informações tornou-se algo vital e a empresas foram

expandindo tal conectividade de seus ambientes internos, para parceiros, fornecedores, clientes e assim por diante (SÊMOLA; 2003). A ampliação das performances de tecnologias de processamento e comunicação, bem como o desenvolvimento de novas rotinas de integração entre os *stakeholders* possibilitou uma ampliação da integração e compartilhamento de informações.

Tal crescimento de conectividade além dos benefícios trazidos pela velocidade de obtenção de informações e serviços associados, também ocasionou a ampliação dos riscos em manter as informações seguras. O que antes era possível apenas com vigilância física de uma sala onde estava localizado o mainframe, atualmente não é suficiente. A possibilidade de acessos remotos utilizando diversos meios de penetração nas bases de dados tornou sua segurança bem mais complexa.

Stair e Reynolds (2002) defendem que, quanto mais a tecnologia torna as organizações e indivíduos velozes, complexos e poderosos, maior é o risco em experimentar erros relacionados à informática. O´Brien (2001) também estabelece o mesmo parâmetro de complexidade com a ampliação da facilidade na cooperação e compartilhamento de recursos. Diante deste contexto, a Segurança da Informação começou a ser um fator importante das gestões organizacionais e configurar-se entre as preocupações dos gestores organizacionais.

Martins (2007) relata os estudos iniciais na área de Segurança da informação, informando que quem primeiro estruturou estudos nesta linha foram os Estados Unidos. Tal autor diz que já na década de 60, iniciaram os primeiros trabalhos com ênfase na Segurança da Informação. Em 1967, nos Estados Unidos, foi publicado um documento intitulado *"Security Control for Computing System: Report of Defense Science Boad Task Force on Computer Security"*, que consistia em um conjunto de normas estabelecidas para práticas de segurança da informação em ambientes computacionais.

Dez anos depois, o Departamento de Defesa dos Estados Unidos formulou um plano sistemático para tratar do Problema Clássico de Segurança, o qual daria origem ao "*DoD Computer Security Initiative*", que, por sua vez, desenvolveria um "Centro" para avaliar quão seguras eram as soluções disponibilizadas. A construção do "Centro" gerou a necessidade da criação de um conjunto de regras a serem utilizadas no processo de avaliação. Este conjunto de regras ficaria conhecido informalmente como "*The Orange Book*", devido à cor alaranjada da capa deste manual de segurança, e o Coronel Roger Shell foi o primeiro diretor deste Centro (MARTINS; 2007). O "*Orange Book*" teve o seu início ainda no ano de 1978 e, mesmo que ele seja considerado ultrapassado, podemos considerá-lo como o marco

inicial de um processo mundial e contínuo de busca de um conjunto de medidas que permitam a um ambiente computacional ser qualificado como seguro.

Com o passar dos anos, foram criadas diversas normas, práticas e sistemas com o objetivo principal de promover a Segurança da Informação nas Organizações. Sêmola (2003) aponta que a preocupação na Segurança da Informação deve existir oficialmente nas organizações. A criação de Comitês Corporativos de Segurança que estão constantemente definindo padrões e monitorando ações e a presença de *Security Office* orientando ações na área tornou-se algo necessário para que as organizações tenham confiança nas suas informações e evitem prejuízos. Além disso, a adoção de normas e padrões nacionais ou internacionais possibilita maior respeitabilidade pelos clientes, fornecedores e demais envolvidos com a organização. Estes aspectos de certificação serão abordados com mais detalhes na seção 2.2 deste estudo.

2.1.2 Conceitos relacionados com a Segurança da Informação

Os princípios da Segurança da Informação são os conceitos que norteiam todas as ações nesta área. Diversos autores, dentre eles, Laureano (2005) descrevem os princípios básicos para garantir a segurança das informações:

- Confidencialidade: a informação somente pode ser acessada por pessoas explicitamente autorizadas; é a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.
- Disponibilidade: a informação ou sistema de computador deve estar disponível a quem possa acessá-la no momento em que a mesma for necessária;
- Integridade: A informação deve ser retornada em sua forma original no momento em que foi armazenada; é a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

Sêmola (2003) alerta a importância de estar atento aos princípios em todos os momentos do ciclo de vida da informação, como ilustrado no diagrama 2, onde ela é estabelecida como cerne por onde são estabelecidos os princípios, a legalidade e autenticidade como formas de garantia da legitimidade da informação. No entorno, aparecem os estágios de

manuseio, armazenamento, transporte e descarte da informação, pois, em todos estes momentos, pode haver falhas de segurança que prejudiquem a organização.

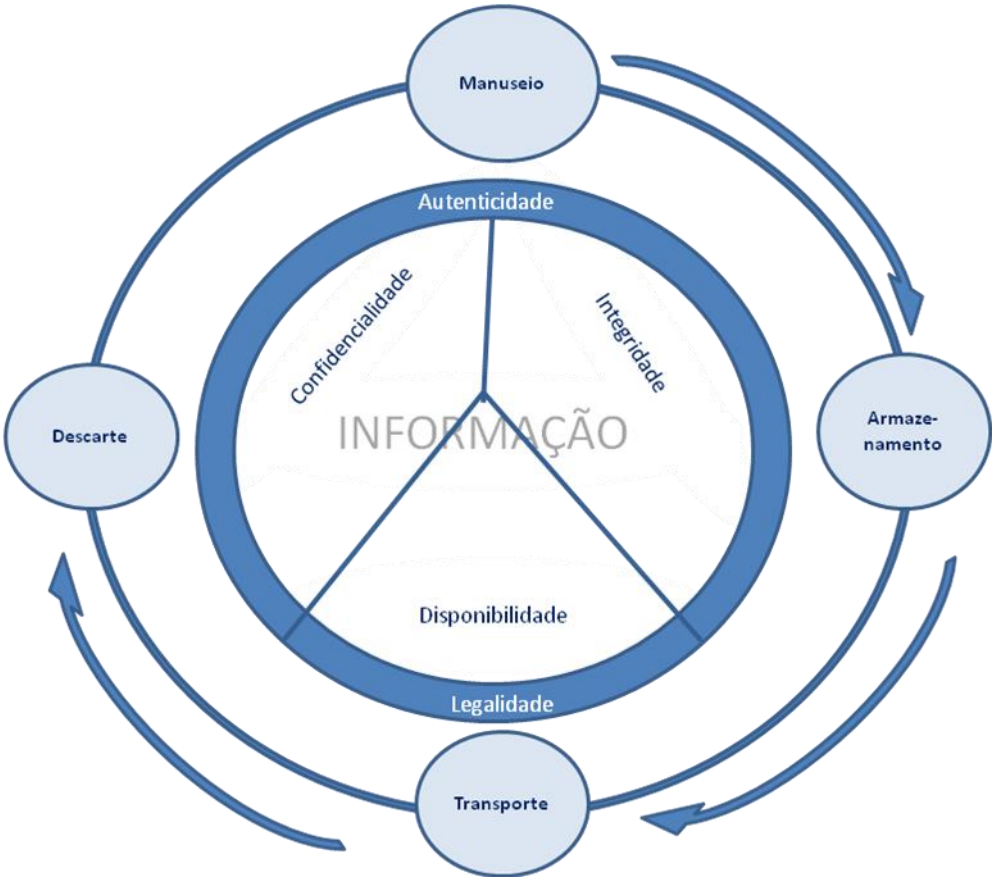


Diagrama 2. Conceitos básicos e aspectos complementares de segurança da informação no ciclo de vida da informação.
Fonte: Sêmola (2003)

O manuseio refere-se a qualquer momento no qual a informação é criada e manipulada, como por exemplo: ler um documento ou digitar uma mensagem. O contato físico ou virtual com as informações caracteriza essa fase. O armazenamento diz respeito ao momento em que a informação é guardada. Após o manuseio, a informação será armazenada, seja em um banco de dados ou transcrita para determinado arquivo físico. O transporte é caracterizado pela forma como a informação é enviada a terceiros ou conduzida pelo seu responsável, como por exemplo: o uso do correio eletrônico ou o seu transporte em mídia (CD, *pendrive* etc.) por intermédio do mensageiro. O descarte trata da maneira como a mensagem é descartada, seja ao depositar a mensagem de papel no lixo ou ao se eliminar um

arquivo eletrônico. Em todos estes momentos a informação está vulnerável e Sêmola (2003) defende que em cada uma das fases do ciclo de vida da informação deve ser dispensado tratamento especial que garanta aspectos ligados à sua segurança.

Considerando os três princípios da segurança, D´Andrea (2004) define que a segurança pode ser estruturada sobre dois imperativos. O primeiro deles preza a segurança em si, garantindo a exclusão de quem é indesejado no ambiente da organização. O segundo, mais focado no principio da disponibilidade, é o habilitador que garante acesso a quem possui este direito. Tal autor afirma ainda que o equilíbrio entre o "proteger" e o "habilitar" garante uma infraestrutura segura e alinhada à missão da organização.

Independente da razão, a preocupação em investir-se em segurança da informação é algo crescente nas organizações e com isto, muitos conceitos foram incorporados ao dia-a-dia de quem trabalha na área, dentre eles podemos destacar os que se encontram no quadro 2. Tais conceitos são detalhados como forma de facilitar a compreensão do instrumento de pesquisa e dos tópicos seguintes deste trabalho.

CONCEITO	DESCRIÇÃO
Ameaça	É algo que oferece risco à organização através de atuação de alguém sobre alguma vulnerabilidade. Segundo Sêmola (2003) elas podem ser classificadas em: naturais (advindas de fenômenos da natureza, como terremotos, enchentes etc.); involuntárias (inconscientes por erros ou acidentes); voluntárias (ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários)
Antivírus	Programa que faz a varredura de arquivos maliciosos disseminados principalmente pela Internet ou correio eletrônico. Basicamente, sua função está atrelada à ponta do processo, isto é, ao usuário que envia e recebe dados. Uma das últimas tendências deste tipo de ameaça são os chamados "vírus polimórficos", que possuem a capacidade de mudar constantemente para driblar a vítima e dificultar sua remoção
Ataque	É a efetivação da ameaça
Ativos	Todo recurso que é precioso para a organização e deve ser protegido de um ataque
Auditoria	Processo de coleta de evidência na utilização de informações. É utilizada para identificar entidades envolvidas na comunicação. Pode resultar, por exemplo, em detecção de falhas ou responsabilização de ataques
Autenticação	São processos de identificação para disponibilizar acesso. A autenticação e conseqüente autorização de manipulação dos dados se baseiam em algo que o indivíduo sabe (uma senha, por exemplo), algo que ele tem (dispositivos como tokens, cartões inteligentes, etc.) e o que ele é (leitura de íris, linhas das mãos etc.)
Balanceamento de carga	As ferramentas de balanceamento estão relacionadas à capacidade de operar de cada servidor da empresa. Elas permitem que, em horários de grande utilização da rede, se determine a hierarquia do que trafega, bem como o equilíbrio da carga disseminada entre os servidores
Criptografia	É utilizada para garantir a confidencialidade das informações. Trata-se de uma codificação que usa um processo de decifração para restaurar os dados ao seu formato original. As chaves criptográficas podem ser simétricas (privada) ou assimétricas (pública)

Detector de Intrusão (IDS)	Estas ferramentas têm a função de monitorar o tráfego contínuo da rede, identificando ataques que estejam em execução. Como complemento do firewall, o IDS (*Intrusion Detection System*) se baseia em dados dinâmicos para realizar sua varredura, como por exemplo, pacotes de dados com comportamento suspeito, códigos de ataque e outros
Divulgação	Exposição de informações confidenciais capturadas de forma desonesta
Elevar privilégios	Alteração de nível de segurança de um usuário para níveis com maior acesso
Falsificação	Quando uma pessoa se passa por outra, por exemplo, utilizar senha de outro usuário de sistema
Firewall	Cumprem a função de controlar os acessos. São soluções que, uma vez estabelecidas suas regras, passam a gerenciar tudo o que deve entrar e sair da rede corporativa. Muitas vezes, recomenda-se a adoção do firewall para separar a intranet da companhia de seus clientes externos ou de servidores e serviços públicos. Basicamente, o firewall é um software, mas também pode incorporar um hardware especializado
Impacto	Abrangência dos danos causados pelo incidente de falha na segurança nos processos de negócio da organização
Incidente	Evento decorrente da ação de uma ameaça causando impactos nos processos do negócio
Integradores	Permite centralizar o gerenciamento de diferentes tecnologias que protegem as operações da rede. Mais que uma solução, trata-se de um conceito
Legalidade	Características de informações que possuem valor legal
Rede Privada Virtual (VPN)	Uma das alternativas mais adotadas pelas empresas na atualidade, as VPN's são canais que utilizam túneis para trafegar dados criptografados entre divisões de uma mesma companhia, parceiros de negócios etc.
Repudiação	Negar a violação/ataque, por exemplo, apagar o *log* (histórico de acessos) de uma máquina
Risco	Probabilidade de perda dos princípios da Segurança (confidencialidade, integridade e disponibilidade) através de ameaças que explorem as vulnerabilidades
Varredura de vulnerabilidades	Produtos que permitem realizar verificações regulares em determinados componentes de rede como servidores e roteadores. O objetivo destas ferramentas é encontrar brechas de sistemas ou configurações
Violação	Alteração de dados
Vulnerabilidades	Pontos susceptíveis a ataque e ameaças, como: roubos de senhas, engenharia social, segurança de dados incorreta, segurança física incorreta e transmissão de dados em criptografia. Podem ser classificadas em diversos tipos, sendo as mais comuns: de hardware, de software, de comunicação e humanas

Quadro 2. Conceitos importantes em segurança da informação
Fonte: Próprio autor (2008)

Ampliando os conceitos explicitados no quadro 2, Nakamura e De Geus (2003) relatam uma classificação mais detalhada das pessoas que acessam informações sem autorização, como: *Script Kiddies* (iniciantes em ataques); *Cyberpunks* (pessoas mais velhas e anti-sociais); *Insiders* (empregados que invadem suas próprias organizações por insatisfação); *Coders* (os que escrevem sobre suas "proezas"); *White hat* ou hackers do bem (profissionais contratados para descobrir vulnerabilidades das organizações e aplicar correções necessárias); *Black hat* (*crackers* que prejudicam ou fazem chantagem com os responsáveis pelas organizações invadidas); *Gray hat* (*hackers* que vivem no limite entre o *white hat* e o *black hat*).

Nakamura e De Geus (2003) ainda definem que aspectos tecnológicos, humanos, processuais, jurídicos e de negócios devem ser levados em consideração para garantir a disponibilidade, integridade e sigilo das informações. Eles reforçam que manter os princípios básicos da segurança da informação em uma organização não se resume a combater *hackers*, maus funcionários ou vírus. Daí extrai-se uma preocupação mais gerencial de tais autores que percebem o perigo não como algo meramente operacional, mas que pode impactar seriamente os negócios da organização.

Como forma de proteção, as organizações utilizam Medidas de Segurança que, segundo Sêmola (2003), podem evitar o incidente antes que ele ocorra (as preventivas), identificar as condições ou indivíduos causadores de ameaças (detectáveis), corrigir uma estrutura tecnológica ou humana para que se adaptem ao ambiente seguro ou reduzir impactos de um dano causado por falta de segurança (as corretivas).

Ferreira (2003) defende ponto de vista semelhante quando relata que a segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades.

Ambos os autores colocam em destaque a importância da Segurança da Informação como fator que permite sucesso às organizações e focam na questão gerencial de decidir até que ponto a proteção não é prejudicial, ou seja, a importância de estabelecer regras de segurança que não tornem o negócio lento e inviável. O gestor também deve estar atento ao fato de que, quanto maior o nível de segurança, mais elevados serão os custos. Assim, a organização deverá avaliar a relação custo/benefício de sua estrutura de segurança.

Apesar desse cuidado que se deve ter na medida de segurança a ser adotada, alguns autores, dentre eles, D'Andrea (2004), Nakamura e De Geus (2003) não consideram a segurança apenas como uma forma de proteção e sim, como elemento habilitador dos negócios da organização, permitindo que ela busque lucro por meio de oportunidade de negócios através da flexibilidade, facilidade e disponibilidade dos recursos de informática.

Outro enfoque, colocado por Fontes (2005), trata dos motivos para que as pessoas não dêem a devida importância à segurança. O autor identificou como principais os seguintes: falta de conscientização; crença de que não é preciso controlar o acesso à informação; crença de que todos os usuários são honestos; crença de que a organização vai gastar dinheiro; crença de que o pessoal da informática resolve tudo; crença de que nunca vai acontecer um desastre na organização; crença de que um *firewall* resolve tudo; e crença de

que segurança é apenas para grandes organizações. Tais motivos podem explicar a resistência de alguns gestores em designar parte do orçamento de suas organizações para esta área.

Cavusoglu, Mishira e Raghunathan (2004) alertam que o medo, a incerteza e a dúvida foram estratégias usadas por vários anos para vender soluções de segurança de dados, no entanto, apontam para um cenário de mudanças nesta área, no qual, a metodologia para análise de investimentos em segurança é feita de forma mais racional.

Ferreira (2003) define que um bom planejamento é um passo inicial a um programa de segurança bem sucedido e propõe as seguintes questões como análises iniciais: O que devemos proteger? Contra o que ou quem? Quais as ameaças mais prováveis? Qual a importância de cada recurso? Qual o grau de proteção desejado? Quanto tempo, recursos humanos e financeiros pretendemos gastar para atingirmos os objetivos de segurança desejados? Quais as expectativas dos usuários e clientes em relação à segurança das informações? Quais as consequências para a organização se os sistemas de informação forem corrompidos ou roubados?

Após o conhecimento inicial da situação proposto por Ferreira (2003), é importante estabelecer estratégias de defesa dos ativos organizacionais. Segundo Turban, Rainer e Potter (2003), as principais estratégias de defesa são: Controle para prevenção e desencorajamento; Detecção; Controle de danos; Recuperação e Correção.

Tais autores classificam os controles como gerais e de aplicação, sendo que os gerais são detalhados em cinco categorias, a saber: Físicos; Acesso (Biometria por Geometria da mão; Padrão de vasos sanguíneos da retina do olho; Voz; Assinatura; Dinâmica de uso de teclas; Reconhecimento facial; Impressões digitais - imagens dos dedos; Varredura da íris); Segurança de dados; Comunicação (redes); e Administrativos. Na mesma linha de Turban, Rainer e Potter (2003), Sêmola (2003) descreve a Teoria do Perímetro, que aponta para a delimitação do espaço a ser considerado e descreve seis barreiras principais que devem ser utilizadas pelo Gestor de Segurança da Informação, conforme apresentado no diagrama 3.

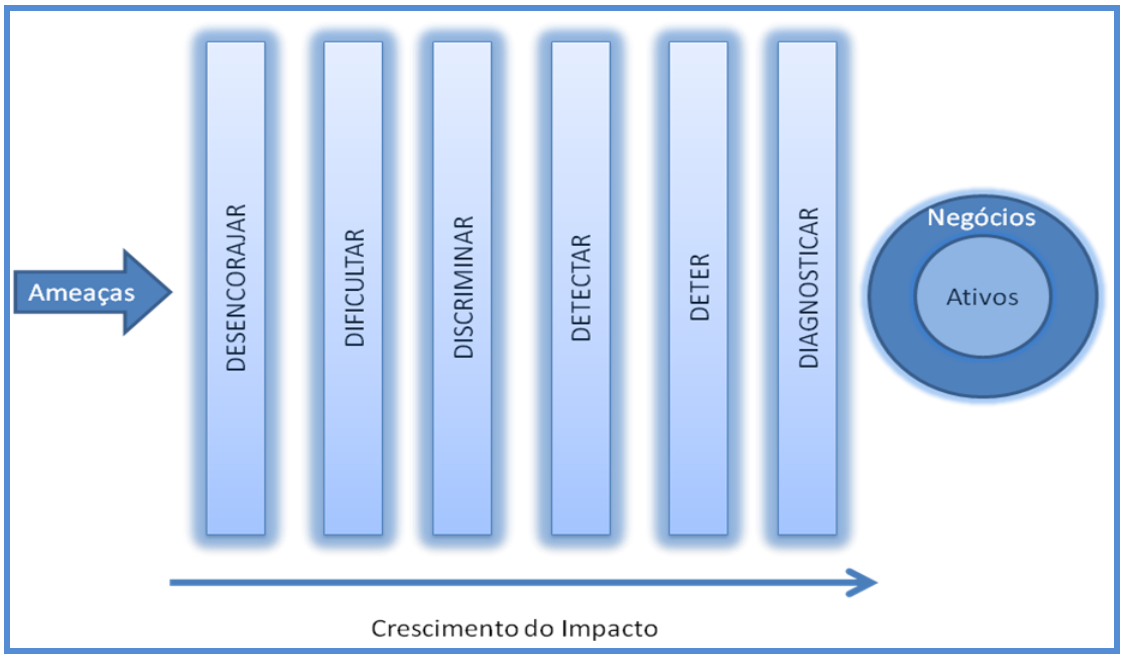


Diagrama 3. Barreiras da Segurança.
Fonte: Sêmola (2003)

A primeira barreira apresentada no Diagrama 3 representa as ações que podem ser realizadas no sentido de desencorajar as ameaças, como por exemplo, a colocação de uma câmera. A segunda barreira pode ser adotada como forma de dificultar o acesso, como a colocação de dispositivos de autenticação e reconhecimento. Estabelecer os limites de acesso de um email é uma forma de adoção da terceira barreira (discriminar). A detecção de situações de risco é a quarta barreira. A quinta barreira busca impedir que as ameaças atinjam seus objetivos. A última barreira retroalimenta o ciclo, permitindo subsídios de ajustes da primeira barreira. Percebe-se que todas as barreiras são complementares e o trabalho contínuo do gestor em tais barreiras permite maior segurança aos ativos informacionais da organização.

A gestão de tais barreiras deve estar alinhada com a Política de Segurança da Informação, que é um conjunto de regras que devem nortear a empresa. Ela deve estar intrinsecamente relacionada à missão e a visão de futuro da organização, além de ser acatada por todos os que fazem parte da organização, ser de fácil compreensão, ter comprometimento da alta cúpula da organização. Nele deve existir a previsão de atitudes em diversos casos, até mesmo na perda dos dados, com a adoção de estratégias de contingência.

As principais estratégias de contingência são o *hot-site* (pronta para entrar em ação em frações de milissegundos), *warm-site* (adotada quando o retorno da operação pode demorar mais que os primeiros, sem causar impactos significativos), realocação de operação

(alteração de ambiente físico para outra estrutura similar), bureau de serviços (semelhante ao anterior, sendo que o ambiente de realocação utilizado é terceirizado), acordo de reciprocidade (adoção de ambientes de duplicidade em outra organização que também utiliza o ambiente da organização demandante), *cold-site* (adota recursos mínimos de contingência), auto-suficiência (quando não se pode adotar as anteriores).

A adoção de tais estratégias também é confirmada por D´Andrea (2004) que define que o processo de construção de uma plataforma segura deve ser estruturado e composto das seguintes etapas: Entendimento do valor e contribuição que a segurança pode proporcionar à organização; Análise de fatores externos que possam interferir na segurança; Identificação dos fatores estratégicos que possam causar algum impacto no planejamento ou na implantação da segurança da organização; Adoção de um modelo abrangente que permita identificação e demonstração do valor que a segurança pode trazer à organização; Definição de um conjunto de soluções integradas com a criação de um plano estratégico de segurança.

Uma ação importante que deve compor o planejamento estratégico da segurança é a divulgação, pois a segurança não pode se basear apenas em aspectos tecnológicos. Segundo D´Andrea (2004), os pilares da segurança estão fundamentados em tecnologia, processos e pessoas. O advento da internet trouxe mais riscos de segurança para empresa e estes três pilares devem ser consistentes e seguros para evitar prejuízos à organização. Tal autor argumenta que, sem as regras, as responsabilidades e os procedimentos dos processos, bem como, sem as pessoas necessárias por gerir tais processos, investir em tecnologia pode resultar em um fracasso muito caro. Daí a importância da decisão gerencial para que as ações de Segurança da Informação estejam fundamentadas em regras consistentes, alinhadas ao negócio da organização e possam atingir suas metas.

Com a adoção de estratégias de defesa eficientes, as organizações pretendem obter: Maior padronização das informações e processos; Alinhamento dos objetivos do órgão com as leis e obrigações contratuais; Definição dos responsáveis pelos ativos do órgão; Definição das penalidades pela não aderência à Política de Segurança; Aumento da conscientização da empresa; Aderência aos padrões internacionais de gestão de segurança; Segurança dos processos do negócio; Retorno do investimento por meio de redução de acidentes; e Consolidação da imagem de uma empresa segura (TURBAN; RAINER; POTTER, 2003).

Uma máxima bastante comum na área de segurança é: “uma corrente é tão forte quanto seu elo mais fraco”. Assim o reforço nos três pilares (tecnologia, processos e

pessoas) deve ser proporcional, evitando uma estrutura de segurança muito rígida em um dos pilares e muito fraca em outro, permitindo suscetibilidades a ataques.

2.1.3 Segurança da informação no setor público

O CERT (*Computer Emergency Response Team*) é uma organização norte-americana criada em 1988 com o objetivo de monitorar a segurança na internet e coordenar a atuação de agências autorizadas na fiscalização realizada na rede mundial de computadores (STAIR; REYNOLDS, 2002). Tal órgão foi financiado em parte por universidades e conta com um pequeno grupo de funcionários altamente qualificados. Em sua pesquisa anual mais recente, referente ao exercício de 2008, destacam-se incidentes de Segurança da Informação no âmbito de governos dentre os mais críticos. Tal organização ainda relata que o governo dos Estados Unidos da América está percebendo que a proteção de sua infraestrutura informacional é um imperativo nacional (CERT; 2009).

A preocupação das organizações públicas nesta área também pode ser percebida na última edição da Pesquisa Nacional de Segurança da Informação realizada pela empresa *Modulo Security* em 2006 (MODULO; 2009) no Brasil, onde 21% das empresas entrevistadas faziam parte do segmento de governo. Tal pesquisa apresentou um perfil da situação das empresas em termos de falhas de segurança, destacando que: 33% dos gestores não sabem quantificar as perdas e 48% não sabem identificar os responsáveis pelos problemas; 25% tomam providências internas, acionando por conta própria o causador do problema; em 24% dos casos de falhas de segurança, elas são causadas por funcionários internos e 20% por hackers; os problemas que mais causam danos financeiros são vírus (15%), spam (10%) e fraudes (8%); 77% dos gestores acreditam que os problemas relacionados à Segurança da Informação aumentarão; a maioria dos entrevistados (55%) considera a falta de conscientização dos executivos e usuários o principal obstáculo para a implementação da segurança na empresa, seguido de 28% que alegam falta de orçamento; o maior motivador para a adoção de práticas de segurança é o nível de consciência dos executivos e usuários (31%).

Além disso, a referida pesquisa concluiu que as organizações do Governo são as que menos quantificaram as perdas causadas por problemas de segurança, uma vez que

56% delas não sabem dizer em quanto ficou o prejuízo causado por ataques e invasões. No setor Comércio, 26%; no setor Financeiro, 24%; e no setor Indústria, 36%.

Miranda e Streit (2007) asseguram que a gestão da informação em organizações públicas é mais complexa por necessitar de prestação de contas da tomada de decisão e transparência com fluxo confiável. Tal afirmação reforça a importância de uma Gestão de Segurança da Informação voltada para melhores práticas, já que sem tal gestão amplia-se o risco de ataques e perdas que podem causar prejuízos aos cofres públicos.

Outro fator preponderante é o aumento da demanda de serviços que exigem alto grau de confiabilidade e segurança, como os apontados pelo anuário da revista TI & Governo (PLANO EDITORIAL; 2005) como principais investimentos dos governos estaduais e federal na área de TI para o ano de 2006 aplicativos de VoIP e redes sem fio (*wireless*). Tais destaques demonstram uma tendência em investimentos de telecomunicações que precisa ser suportada por uma estrutura segura para evitar prejuízos ao erário público e danos à população.

Nas organizações do setor público, as seguintes falhas podem trazer perdas ao patrimônio por: Ataques físicos (roubos ou danificação de equipamentos); Ataques lógicos (adulteração de dados financeiros, exclusão de multas, adulteração de valores de pagamentos etc.); Perda de credibilidade da mesma forma que para empresas privadas. Oliveira (1994) prega que o atual modelo resultante da era industrial, onde o Estado (setor público) possui poderes normativos e isentos, está em declínio; com isso, o papel do Estado passa a ser muito parecido com o da iniciativa privada, pois o setor público passa a ter preocupações de competitividade.

Apesar de tal apontamento alertando para a tendência de similaridade entre ambos os setores (público e privado), como as organizações públicas têm o papel de servir toda a sociedade, os prejuízos podem ter repercussões bem maiores e causar prejuízos mais amplos porque atingem os interesses de todos os cidadãos. Além disso, a agilidade em processos de aquisição deve ser considerada, já que na área pública a tramitação de processos desta natureza costuma ser mais lenta pelas exigências legais. Isso pode resultar em sérios problemas na segurança se não houver uma gestão adequada.

2.2 MODELOS DE CERTIFICAÇÃO EM SEGURANÇA DA INFORMAÇÃO

O Tribunal de Contas da União do Brasil justifica a utilização de Práticas Avançadas em Segurança da Informação, pela importância da informação para qualquer organização (TCU-BRASIL, 2008, p.26), conforme a seguir:

> a informação é um ativo muito importante para qualquer organização, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da organização perante terceiros, como também o andamento dos próprios processos organizacionais. É possível inviabilizar a continuidade de uma organização se não for dada a devida atenção à segurança de suas informações.

Existem diversas técnicas e métodos de boas práticas que são utilizados pelas organizações para promover Segurança da Informação. Os mais citados são resumidos a seguir em ordem cronológica.

O Trusted Computer Security Evaluation Criteria (TCSEC) foi publicado pela primeira vez em 1985 pelo Departamento de Defesa Norte-americano e serviu como base para outros modelos criados na Europa e Canadá. Este modelo foca em critério de funcionalidade, efetividade e garantia (ou confiabilidade). Ficou conhecido popularmente como Livro Laranja (*Orange Book*) devido à cor da capa de sua publicação. Sua versão corrente é datada de 1985. Algumas mudanças foram feitas em 1990 para uma possível troca de versão, mas não foi formalmente adotada.

O TCSEC leva em consideração cinco aspectos de segurança: a) a política de segurança do sistema; b) os mecanismos de contabilidade/auditoria do sistema; c) a operacionalidade do sistema de segurança; d) o ciclo de vida do sistema de segurança; e) a documentação desenvolvida e atualizada sobre os aspectos de segurança do sistema

O nível de segurança TCSEC indica se um computador possui um conjunto pré-definido de características de segurança e eles são classificados por letras que variam de D (mínimo de proteção) a A (máximo de proteção), conforme descrito no quadro 3.

NÍVEL	DESCRIÇÃO
D	**Mínimo de Proteção** (Qualquer sistema que não se enquadre em outra categoria ou que não tenha recebido um nível maior de classificação. Computadores Pessoais baseados no sistema DOS são enquadrados nesta categoria)
C	**Proteção Discreta** (Neste nível estão os Trusted Computer Bases - TCBs com proteção de objetos. Ex.: arquivos, diretórios, dispositivos etc.)
C1	**Proteção de Segurança Discreta** (proteção de arquivo opcional; proteção por senha; sistemas que operam em modo de segurança; checagem de integridade do TCB; Documentação de segurança para usuários, para administradores do sistema, para testes de segurança. Exemplo: versões iniciais do UNIX)
C2	**Proteção de Acesso Controlado** (além de todas as características do nível C1, também possui possibilidade da proteção de objetos ser realizada por usuários simples; somente usuários autorizados podem ter acesso; proteção na reutilização de objetos; utilização de identificação e autorização para usuários; auditoria dos eventos de segurança e de dados; operação do sistema em modo protegido; documentação do nível C1 mais informações sobre análise de auditória. Exemplo: últimas versões de UNIX, VMS.)
B	**Proteção Obrigatória** (Neste nível a proteção de sistemas TCB é obrigatória)
B1	**Proteção de Segurança Rotulada** (além de todas as características do nível C2, a segurança é obrigatória para acesso a objetos; é realizada checagem da integridade de rótulo; são feitas auditoria dos rótulos dos objetos; o controle de acesso obrigatório; os recursos para especificar níveis de segurança para documentos que estão em fila de impressão).
B2	**Proteção Estruturada** (além de todas as características do nível B1, possui notificação de alterações nos níveis de segurança que afetam os usuários; rótulo de dispositivos hierárquicos; acesso obrigatório aos objetos e dispositivos; comunicação segura entre usuários e sistema; cobrir armazenamento de canais; permite que o sistema opere em múltiplos níveis, análise e auditorias de versão, atualização e correções; dentre outras. Exemplo: Honeywell Multics)
B3	**Domínio Seguro** (além de todas as características do nível B2, ACLs adicionais para grupos e identificadores; caminho de acesso e autenticação confiáveis; análise de segurança automática; modelo de TCB mais formal; auditoria da analise de eventos seguro; recuperação segura após o sistema cair e documentação relevante; zero erros na TCB e o mínimo de implementações com falhas.
A	**Proteção Verificada** (Este é o nível mais alto de segurança)
A1	**Proteção Verificada** (todas as características do nível B3 mais métodos formais e aprovado da integridade da TCB)
A e outros	Existem previsões para níveis superiores ao A2 embora ainda não estejam formalmente definidos.

Quadro 3. Níveis de segurança conforme TCSEC
Fonte: DOD (2008)

Após a publicação do TCSEC pelos Estados Unidos da América, a Comissão das Comunidades Européias publicou o *Information Technology Security Evaluation Criteria* (ITSEC), que é outro padrão ou conjunto estruturado de critérios para avaliar a segurança de computadores de acordo com produtos e sistemas.

O ITSEC foi publicado pela primeira vez em maio de 1990 na França, Alemanha, Países Baixos e Reino Unido com base em trabalhos existentes em seus respectivos países, realizados especialmente por dois órgãos britânicos, o DTI (*The Department of Trade and Industry*) e o GCHQ (*Government Communications Headquarters*). Após extensa revisão internacional, a versão 1.2 foi posteriormente publicada em junho de 1991 pela Comissão das Comunidades Européias para a utilização operacional dentro de avaliação e de sistemas de certificação.

Desde o lançamento da ITSEC em 1990, uma série de outros países europeus reconheceram a validade das avaliações ITSEC, no entanto, ele tem sido amplamente substituído por critérios comuns, que preveem níveis de similarmente definidos para avaliação e implementação do conceito Alvo de Segurança.

Neste padrão, o produto ou sistema a ser avaliado (chamado a meta de avaliação), é submetido a um exame detalhado de suas características de segurança, resultando em informações funcionais e testes de penetração. O grau de análise depende do nível de confiança desejado no alvo. Para proporcionar diferentes níveis de confiança, a avaliação ITSEC define níveis, do E0 ao E6. Maiores níveis avaliação envolvem mais extensa análise e teste do alvo.

European Communities (2008) esclarece que, ao contrário do TCSEC desenvolvido pelo Departamento de Defesa dos EUA, o ITSEC não exige que um determinado critério possua níveis específicos para fornecer autenticação em outro, ou seja, é possível fornecer autenticação para integridade das funcionalidades sem fornecer para a confidencialidade ou disponibilidade.

Canadian Trusted Computer Products (CTCPEC) é o critério de avaliação canadense. Trata-se de uma norma de segurança da informação publicada em 1993 pela Instituição de Segurança das Comunicações para fornecer uma avaliação critérios de produtos TI. É uma combinação dos TCSEC (*Orange Book* dos Estados Unidos) e o padrão descrito pela Comunidade Européia, o ITSEC. Os padrões CTCPEC, ITSEC e TCSEC foram a base para a criação da norma *Common Criteria*.

Common Criteria é outro padrão que consiste de um framework no qual os usuários podem especificar os requisitos de segurança e os laboratórios podem avaliar os produtos para determinar se eles realmente satisfazem as reivindicações.

Em outras palavras, *Common Criteria* prevê a garantia de que o processo de especificação, implementação e avaliação da segurança de um computador ou produto esteja conforme o padrão. Sua primeira versão foi publicada em 2006 como uma tentativa de padronizar os critérios de segurança do ITSEC, CTCPEC (*Canadian Criteria*) e *US Federal Criteria* (FC). O *Common Criteria* define diversos conceitos utilizados pelas várias normas que tentou padronizar. Os mais comuns são detalhados no quadro 4.

CONCEITO	DESCRIÇÃO
Alvo da Avaliação (TOE)	É um conceito adotado neste padrão e representa o produto ou o sistema objeto de avaliação. A avaliação serve para validar as afirmações feitas sobre o alvo.
Perfil de Proteção (PP)	Documento, normalmente criado por um dos utilizadores ou da comunidade, que identifica os requisitos de segurança para uma classe de dispositivos de segurança (por exemplo, *smart cards* utilizados para fornecer as assinaturas digitais de rede ou firewalls) relevante para usuários com finalidades específicas.
Objetivo da Segurança (ST)	Documento que identifica as propriedades de segurança do alvo de avaliação. Pode referir-se a um ou mais PPs. Permite que vendedores adéquem a avaliação para corresponder com precisão às capacidades do seu produto. Isto significa que uma rede firewall não tem de cumprir os mesmos requisitos funcionais como um banco de dados do sistema de gestão, e que os diferentes firewalls podem ser avaliados em relação completamente diferentes das listas de exigências.
Requisito de Segurança Funcional (SFRs)	Especifica à segurança individual, funções que podem ser oferecidas por um produto. O Common Criteria apresenta um padrão de tais funções.
Requerimentos de Garantia de Segurança (SAR)	Descrição das medidas tomadas durante o desenvolvimento e avaliação do produto para garantir o cumprimento das funcionalidades da Segurança.
Nível de Avaliação da Segurança (EAL)	Classificação numérica descrevendo a profundidade e o rigor de uma avaliação. Cada EAL corresponde a um pacote de requisitos de segurança (SAR, veja acima), que abrange o desenvolvimento completo de um produto, com um determinado nível de rigor. Common Criteria enumera sete níveis, com EAL 1 sendo o mais básico (e, portanto, mais barato de implementar e avaliar) e EAL 7 sendo o mais rigoroso (e mais caro).

Quadro 4. Conceitos do common criteria
Fonte: Common Criteria Recognition Agreement (2007)

Os órgãos de certificação em cada país são responsáveis por atestar a adoção de critérios e normas estabelecidos pelos padrões de Segurança da Informação. Os mais conhecidos são:

- No Canadá: o Conselho de Normas do Canadá (SCC);
- No Reino Unido: Serviço de Normas do Reino Unido (UKAS);
- Nos EUA: o Instituto Nacional de Padrões e Tecnologia (NIST) e o Programa de Normas Nacional (NVLAP);
- No Brasil: Associação Brasileira de Normas Técnicas (ABNT).

A Norma ISO/IEC 27001:2005 é uma das mais recentes normas de Segurança da Informação e, por isso foi adotada nesta pesquisa e será detalhada a seguir.

2.2.1 Norma ISO/IEC 27001

A ISO (*International Organization for Standartization*) é uma Organização Internacional que trata de Normalização. Sua sede funciona em Genebra, na Suíça, e ela foi fundada em 1947. Trata-se de uma organização internacional formada por um Conselho e Comitês com membros oriundos da maioria dos países. Seu objetivo é criar normas e padrões universalmente aceitos sobre como realizar as mais diversas atividades comerciais, industriais, científicas e tecnológicas.

Já o IEC (*International Engineering Consortium*) é uma organização sem fins lucrativos fundada em 1944, sustentada por universidades e sociedades de engenharia. O IEC passou por várias mudanças de forma que atualmente é baseada em informação; com perspectiva internacional e vasta seção de engenheiros, gerentes e executivos. Ela funciona basicamente através de parcerias entre as universidades e indústrias promovendo desenvolvimento de pesquisas inovadoras e programas de serviços (IEC; 2008).

Na área de Segurança da Informação, a norma mais recente certificada pelas duas organizações (ISO/IEC) é a 27001 de 2005. Ela resulta da revisão de sua antecessora, a Norma ISO/IEC 17799:2000, que por sua vez está ligada à norma Britânica BS 7799 de 1995. A ISO/IEC 17799:2000 representou um avanço importante em relação a sua precursora pelo fato de ser reconhecidamente como uma Norma Internacional, haja vista que foi estabelecida pela International Organization for Standardization - ISO.

Pode-se destacar um histórico mais recente para chegar-se ao que é atualmente a ISO/IEC 27001 desde 1987. Neste ano, o Departamento de Comércio e Indústria do Reino Unido (*UK Department of Trade and Industry* – DTI) criou o Centro de Segurança de Computação Comercial (*Commercial Computer Security Centre* - CCSC), com a responsabilidade de produzir um código com as melhores práticas de segurança em TI.

A partir do esforço inicial deste órgão, em 1989, foi publicado em conjunto com o Centro de Computação Nacional dos EUA (*National Computing Centre* – NCC) o "Código de Práticas para Usuários" (*Users Code of Practice*). Alguns anos depois, em 1995, foi publicado o Padrão Britânico (*British Standard*), que era a Norma Britânica BS7799:1995. Quatro anos após a versão inicial da BS7799, foi publicada sua versão revisada, a Norma BS 7799:1999, de abril de 1999.

Em 2000, na reunião do Comitê da ISO, as sugestões de diversos países foram discutidas na reunião denominada *Ballot Resolution* em Tóquio. Em tal ocasião, a Norma foi votada e aprovada pela maioria dos representantes, resultando na publicação da Norma ISO/IEC 17799:2000.

Já a série ISO/IEC 27000 é mais recente e passou por ajustes. Ela pretende contemplar todos os aspectos da segurança da informação, diante do contexto atual de mundo globalizado e importância da informação nas estratégias organizacionais. O planejamento das ações relativas à norma deve atender a um conjunto de requisitos que fazem parte de seus capítulos, cada qual abordando um aspecto da segurança da informação.

A série de normas ISO 27000 foi especificamente reservada pela ISO para assuntos de segurança da informação. Com isso, ocorre o alinhamento de uma série de outros padrões, incluindo a ISO 9000 (gestão da qualidade) e ISO 14000 (gestão ambiental). Tal como acontece com estas outras, a série 27000 é preenchida com uma série de normas individuais e documentos. Alguns destes já são bem conhecidos por terem sido publicados. Outros estão programados para a publicação, com numeração final e publicação detalhes ainda a ser determinada. O quadro 5 reflete as principais normas operacionais da série 27000.

NORMA	DESCRIÇÃO
27001	Esta é a especificação de um sistema de gestão da segurança da informação (um SGSI), que substituiu a antiga norma BS7799-2
27002	Este é o número 27000 série padrão do que foi inicialmente a norma ISO 17799 (que em si era anteriormente conhecida como BS7799-1)
27003	Este será o número oficial de uma nova norma destinada a oferecer orientação para a implementação de um SGSI (IS Management System)
27004	Este é o número designado para um novo padrão do sistema de segurança que aborda a informação de gestão de medições e métricas
27005	Esta é a metodologia independente norma ISO de segurança da informação para a gestão de riscos
27006	Esta norma estabelece diretrizes para as organizações que oferecem certificação SGSI

Quadro 5. Normas operacionais da série 27000
Fonte: ISO (2009)

Nesta pesquisa, foi adotada a norma ISO/IEC 27001, que foi publicada em outubro de 2005 e seu objetivo é proporcionar um modelo para a criação, aplicação, funcionamento, acompanhamento, revisão, manutenção e melhoria do Sistema de Gestão da Segurança da Informação.

Como outras normas da ISO, a 27001 envolve um processo de auditoria em três etapas:

- A Etapa 1 é uma revisão macro da existência de documentação chave, ou seja, como se a organização possui Política de Segurança e Planos de Contingência.
- A Etapa 2 constitui exames mais detalhados, em profundidade envolvendo testes de auditoria, existência e eficácia dos controles de segurança da informação indicados nos planos, bem como sua respectiva documentação.
- A Etapa 3 é uma auditoria posterior para confirmar que uma organização certificada anteriormente continua em conformidade com a norma. Toda Certificação ISO envolve revisões periódicas para confirmar que sistema continua a operar como especificado pela norma.

O processo de certificação começa quando a organização toma a decisão de adotar a norma. A International Organization For Standartization (2009) defende que é evidente que, neste momento, também é importante assegurar o compromisso da gestão, pois a adoção da norma é uma decisão estratégica. Em seguida, deve-se atribuir responsabilidades para o projeto. Uma política organizacional pode ser desenvolvida e publicada, apoiada por políticas setoriais.

A próxima etapa é particularmente crítica. Trata-se da definição do escopo. Normalmente, nesta fase será definida a localização, bens e tecnologias que serão incluídos na política. Nesta fase uma avaliação de risco será realizada, a fim de determinar o perfil da organização quanto à exposição de risco e melhor forma de atuação. O documento produzido será a base para a próxima fase, que será a gestão de tais riscos. Ainda nesse processo será feita uma seleção dos controles adequados em relação aos apresentados na norma, com a justificativa de cada decisão registrada em uma Declaração de Aplicabilidade (SOA). A partir daí, o processo de certificação propriamente dito inicia com avaliação realizada por auditores. Do processo de certificação, pode-se extrair que ele não é apenas um exercício temporário para obter um certificado. Ele deve ter um monitoramento contínuo.

A norma define o seu "processo de abordagem" empregando o modelo PDCA (Plan-Do-Check-Act) para os processos, e reflete os princípios enunciados nas orientações OECD (ISO; 2009). Tal modelo ilustrado no diagrama 4 representa as seguintes fases:

- “Plan” (Planejar) significa estabelecer o Sistema de Gestão de Segurança da Informação - SGSI, a política, objetivos, processos e procedimentos relevantes para a gestão de riscos e a melhoria da segurança da informação com vistas a produzir resultados de acordo com as políticas e objetivos globais de uma organização.

- “Do” (Executar) significa implementar e operar o SGSI, as políticas, controles, processos e procedimentos do SGSI.
- “Check” (Checar/Monitorar/Analisar Criticamente) significa avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiências práticas do SGSI e apresentar os resultados para a análise crítica pelos gestores.
- “Act” (Ajustar/Agir) significa manter e melhorar o SGSI, executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

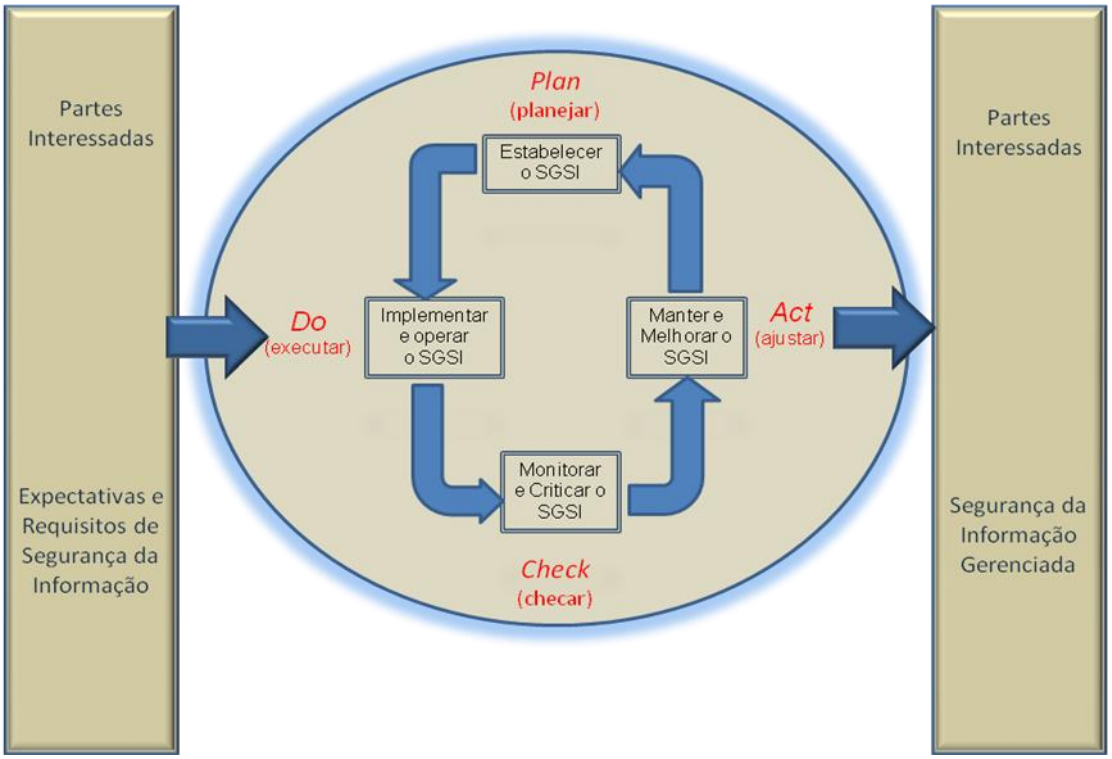


Diagrama 4. Modelo de PDCA aplicado a processos de SGSI
Fonte: ISO (2009)

Conforme detalhado no diagrama 4, verifica-se que o processo de implementação de um Sistema de Gestão de Segurança da Informação, através da adoção de melhores práticas seguindo normas internacionais, possui etapas que devem ser acompanhadas para ser bem sucedido. Além disso, o fluxo é cíclico, tornando necessárias

ações de monitoramento contínuo.

A Norma ISO/IEC 27001:2005 é composta das seguintes seções: a) Gestão de Responsabilidade; b) Auditorias internas; c) Melhorias para SGSI; d) Anexo A - Objetivos dos controles e controles; e) Anexo B - princípios da OCDE e norma internacional; f) Anexo C - Correspondência entre ela e a ISO 9001 e ISO 14001. Em relação aos padrões anteriores, a norma ISO 27001:2005 trouxe algumas alterações que são detalhadas no apêndice E desta pesquisa.

Os objetivos de controle também conhecido como domínios detalhados no anexo A da referida norma são divididos nas seguintes áreas: Política de Segurança (A5); Organização da Segurança da Informação (A6); Gestão de Ativos (A7); Gestão de Recursos Humanos (A8); Segurança do Ambiente Físico (A9); Gerenciamento de Comunicação e Operação (A10); Controle de Acesso (A11); Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (A12); Gestão de Incidentes (A13); Gestão de Continuidade do Negócio (A14) e Aderência (A15). O quadro 6 resume o enfoque de cada um destes domínios.

Domínio	Nome	Recomendações
A5	Política de Segurança	As políticas de segurança da informação devem estar formalmente estabelecidas e serem revisadas em intervalos planejados
A6	Organização da Segurança da Informação	É dividida em responsabilidades internas e externas. Em relação à parte interna, a norma estabelece critérios sobre a clareza nas responsabilidades relativas à Segurança da Informação, bem como, se há participação das diferentes áreas da organização, contatos com autoridades, dentro outras. Já na parte externa, recomenda-se a verificação dos limites de acesso a clientes e usuários externos à organização
A7	Gestão de Ativos	É dividida em responsabilidade pelos ativos e nível de classificação dos mesmos. Estas recomendações visam garantir que os ativos sejam preservados, catalogados e tratados de acordo com seu nível de importância para a organização.
A8	Gestão de Recursos Humanos	Esta seção é dividida em três partes: a primeira relata recomendações de atitudes a serem adotadas antes da contratação dos funcionários para a organização; a segunda trata dos funcionários contratados; e a terceira trata de funcionários que já deixaram a organização.
A9	Segurança do Ambiente Físico	É dividida em áreas de segurança e equipamentos de segurança. Esta seção prevê utilização de controles físicos de acessos e equipamentos para registro dos acessos realizados.
A10	Gerenciamento de Comunicação e Operação	Esta seção é dividida em dez partes: procedimentos operacionais e responsabilidades; gerenciamento de entrega de serviço terceirizado; planejamento e adoção de sistemas; proteção contra códigos maliciosos e móveis; back-up; gerenciamento de segurança da rede; manipulação de mídia; informações trocadas com ambiente externo; serviços de comércio eletrônico; monitoramento.

A11	Controle de Acesso	É dividida em sete partes: normas de controle de acesso; gerenciamento dos usuários; responsabilidades dos usuários; controle de acesso em rede; controle de acesso em sistema operacional; controle de acesso em aplicativos e informação; computação móvel.
A12	Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	É dividida em seis partes: especificações (requerimentos); processamentos de aplicações; controle de criptografias; segurança de arquivos; segurança no desenvolvimento e suporte; gerenciamento de vulnerabilidades técnicas. Estas recomendações visam prevenir falhas de segurança em todas as fases do ciclo de vida de um sistema e sua operação
A13	Gestão de Incidentes	Possui duas partes: relatando eventos (incidentes); e, gerenciamento de incidentes e realização de melhorias
A14	Gestão de Continuidade do Negócio	Apresenta recomendações que visam a continuidade dos negócios da organização, como planos de contingência, por exemplo.
A15	Aderência	É dividida em três partes: aderência com questões legais; aderência com política de segurança e padrões técnicos; e, maximizar eficácia de auditorias de sistemas.

Quadro 6. Domínios da norma ISO 27001
Fonte: ISO (2005)

Para efeito desta pesquisa foram consideradas práticas relativas aos capítulos ou domínios da norma referentes à Controle de Acesso (A11) e Recursos Humanos (A8). Tal escolha justifica-se com base no fato de que tais premissas são geralmente as primeiras trabalhadas na implementação de uma política de segurança e suas práticas são facilmente compreensíveis por público especialista em TI ou não, que é o que se pretende atingir com este trabalho. Assim, procurou-se eliminar o viés de grande número de respostas do tipo "desconheço" por parte dos respondentes que não são da área de TI.

2.3 MODELOS DE ACEITAÇÃO DE TECNOLOGIA

Além dos conceitos de Segurança da Informação apresentados, é importante destacar como outro pilar teórico deste trabalho os modelos de aceitação de tecnologia, haja vista que a pesquisa estuda os fatores de influenciam a **aceitação** de práticas relacionadas à tecnologia da informação.

O modelo *Task-Technology Fit* (TTF) proposto por Goodhue e Thompson em 1995 sugere que a adoção de tecnologia depende em parte do alinhamento entre a tecnologia e as exigências da tarefa em particular. Tal modelo defende que o grau de ajuste da tecnologia é

afetado pelas interações entre as características das tarefas, funcionalidades da tecnologia e personalidade dos usuários, ou seja, as tecnologias podem ter impacto positivo no desempenho quando são utilizadas e quando se ajustam às tarefas realizadas (CARVALHO; FERREIRA, 2005).

Os principais fatores analisados pelo modelo TTF são a qualidade, a localização, autorização, compatibilidade, pontualidade da produção, estabilidade dos sistemas, facilidade de uso, relacionamento do setor de TI com usuários. Assim, tal modelo permite verificar a correspondência destes fatores com diversas dimensões sob a ótica da melhoria de performance do usuário da TI.

Löbler, Visentini e Vieira (2006) utilizam o modelo TTF combinado a outro modelo (TAM - *Technology Acceptance Model*), por considerar que o TTF amplia o segundo modelo, pois a tarefa executada afeta o uso. Tais autores descrevem o TTF da seguinte forma:

> O modelo TTF é uma combinação entre a tarefa e a tecnologia e o consequente uso dessa tecnologia. [...]. Estando ajustada a tarefa e tecnologia, esta explicará a facilidade de utilizar, a intenção de usar e a utilidade percebida. A utilidade percebida implica na intenção de uso, e essa última implica no uso da atual tecnologia (LÖBLER; VISENTINI; VIEIRA, 2006).

Outro modelo bastante testado foi proposto em 1992 por Delone e McLean. Trata-se do *Information System Success* (ISS) que relaciona a qualidade do sistema e da informação com o uso do sistema e a satisfação do usuário, relacionando-as com o impacto individual e organizacional.

Já o modelo *Technology Readiness Index* (TRI – índice de prontidão para o uso de tecnologia) foi desenvolvido por Parasuraman e Colby em 2001 para medir a prontidão de uso de tecnologia pelo consumidor norte-americano. Ele é baseado nos seguintes construtos: otimismo (visão positiva da tecnologia); inovatividade (tendência de ser pioneiro); desconforto (sentimento de estar sendo pressionado pela tecnologia) e insegurança (desconfiança da tecnologia e ceticismo nas habilidades de utilizá-la).

Os dois primeiros construtos do TRI (otimismo e inovatividade) podem ser descritos como facilitadores, ou seja, indutores positivos para a adoção de novas tecnologias e os dois últimos (desconforto e insegurança) são percebidos inibidores ou fatores que podem retardar a adoção de novas tecnologias.

Costa Filho e Pires (2005) utilizam o modelo TRI combinado a outro modelo (TAM - *Technology Acceptance Model*), de forma que os quatro construtos do TRI são analisados como fatores que interferem na intenção de uso de novas tecnologias.

Um dos modelos mais conhecidos e testados é o modelo TAM – *Technology Acceptance Model*. Ele já foi testado em vários tipos de organizações e para as mais diversas áreas, conforme demonstrado no quadro 7.

Ano	Autor(es)	Área de Pesquisa
1996	VENKATESH; DAVIS	Estudo de caso replicado em três organizações
	VENKATESH	Estudo de caso replicado em três organizações
2000	MORRIS; VENKATESH,	Interferência da idade na adoção de tecnologias
2003	DIAS; ZWICKER; VICENTIN	Análise do próprio modelo TAM e suas limitações
	GABBAY	Segurança da Informação
	CAVALCANTE	Segurança da Informação
2004	BUENO; ZWICKER; OLIVEIRA	Comércio Eletrônico
	COSTA FILHO; PIRES	Terminais de autoatendimento (ATM)
	OLIVEIRA; JOIA	Comércio Eletrônico
	SANTOS; AMARAL	Informação *online*
2005	ALMEIDA; SOBRAL	Psicologia
	COSTA FILHO; PIRES CARVALHO; FERREIRA	Psicologia (TAM associado ao TRI) Portais e intranet
2006	PIRES; YAMAMOTO; COSTA FILHO	VoIP
	SILVA; DIAS	ERP
	LÖBLER; VISENTINI; VIEIRA	Comércio Eletrônico
	RODRIGUES; COSTA	Psicologia (modelo conceitual)
2007	OLIVEIRA JUNIOR	Sistemas Integrados de Gestão
2008	OLIVEIRA; RAMOS	*E-learning*
	SILVA; DIAS; SENA JUNIOR	Cultura Organizacional
	SILVA	Biblioteca Virtual
	VASCONCELOS	*E-learning*
2009	NIÑO	Turismo – Comércio *online* e *offline*

Quadro 7. Trabalhos correlatos em modelos de aceitação de tecnologia
Fonte: Próprio autor (2009)

O modelo TAM além de utilizado em diversas áreas de atuação para verificar aceitação de tecnologias, também é utilizado de forma combinada com outros modelos ou ampliado por diversos autores para testar hipóteses. Seus construtos estão em constante avaliação e testes.

Um pressuposto essencial do Modelo TAM baseia-se nos fundamentos da Teoria de Ação Racional (*TRA – Theory of Reasoned Action*) de que parte significativa do comportamento humano tem fundamento racional que o torna previsível pela intenção de agir (ALMEIDA; SOBRAL, 2005; QUINTELLA; PELICCIONE, 2006). A base teórica do TAM inclui conceitos de diversas áreas comportamentais como Psicologia, Sociologia e Gestão

Organizacional (SANTOS; AMARAL, 2004). A TRA foi desenvolvida por Martin Fishbein e Icek Aizen entre 1975 e 1980. O diagrama 5 apresenta as relações dos elementos de tal modelo que afetam o comportamento do indivíduo.

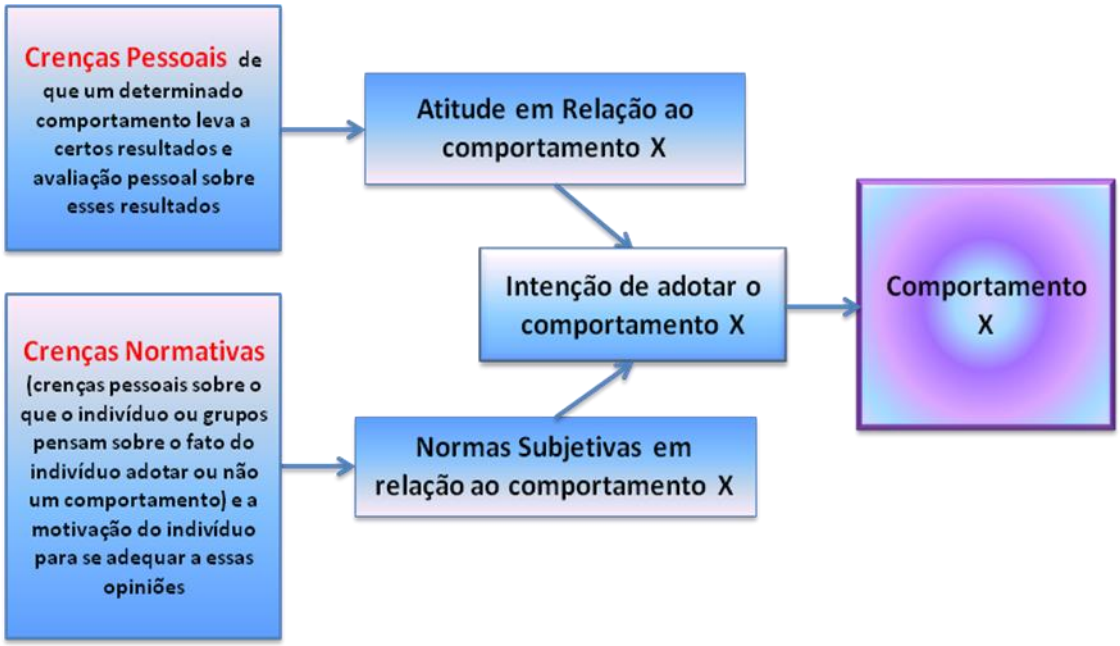


Diagrama 5. TRA – teoria da ação racional
Fonte: Quintella e Peliccione (2006)

A TRA também traduzida como Teoria da Ação Intencional ou Teoria da Ação Fundamentada é um modelo da Psicologia Social que permite analisar os fatores determinantes no comportamento consciente intencional. Segundo tal modelo um comportamento deriva de uma intenção que por sua vez deriva de atitudes e normas subjetivas. Estas atitudes e normas subjetivas resultam em crenças e motivações para o determinado comportamento.

Para a TRA as crenças se referem a informações que um sujeito possui a respeito de um determinado objeto, ligando um determinado objeto a atributos. Tal modelo utiliza as crenças como base para a formação de atitudes.

Já as normas subjetivas se referem à percepção do indivíduo acerca da opinião dos demais em relação ao seu comportamento. Desta forma, a Teoria da Ação Intencional (TRA) entende que a intenção é definida pela probabilidade de um indivíduo comportar-se de determinada maneira.

Algumas lacunas da TRA podem ser preenchidas pela Teoria do Comportamento Planejado (*TPB – Theory of Planned Behaviour*) proposto por Ajzen em 1991. Esta teoria acrescenta aos pressupostos da TRA, a influência das percepções sobre o ambiente para os usuários de tecnologias (ALMEIDA; SOBRAL, 2005), ou seja, a TPB acrescenta um elemento à TRA que é o controle percebido, definido como a percepção individual do seu controle sobre a performance do comportamento. Considera-se esta Teoria como uma extensão à TRA (QUINTELLA; PELICCIONE, 2006).

O modelo original TAM foi desenvolvido por Davis em sua tese de Doutorado em 1986 (DIAS; ZWICKER; VICENTIN, 2003). A proposta deste modelo é traçar o impacto de variáveis em crenças, atitudes e intenções. O modelo proposto por Davis baseia-se em cinco construtos que interferem na aceitação de tecnologias, conforme diagrama 6.

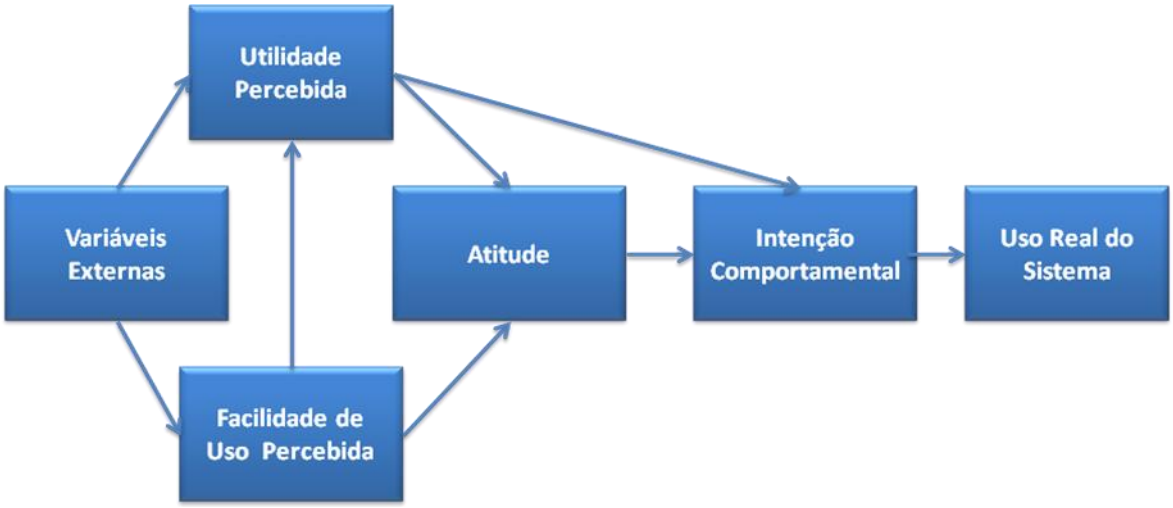


Diagrama 6. Relação dos construtos do modelo TAM
Fonte: VENKATESH (2009)

O TAM se sustenta em dois construtos baseados na crença, que são a *facilidade de uso percebida* e a *utilidade percebida*. A **facilidade de uso percebida** se refere à expectativa do usuário de tecnologia na isenção de esforço físico ou mental com seu uso. Para testar tal construto é comum utilizar perguntas do tipo: Eu acho fácil usar o sistema? Interagir com o sistema requer pouco esforço? (DIAS; ZWICKER; VICENTIN, 2003).

A **utilidade percebida** pode ser definida como uma probabilidade verificada de que desempenho do usuário de tecnologia aumente com sua utilização (COSTA FILHO;

PIRES, 2005). Este construto é testado com perguntas do tipo: Eu acho o sistema útil para meu trabalho? Usar o sistema melhora minha eficiência no trabalho?

O modelo TAM permite a análise da relação entre a *facilidade de uso percebida* e a *utilidade percebida* com outros construtos. O construto **atitude** é definido como um sentimento individual (positivo ou negativo) em relação a um comportamento que se tenha. Oliveira Junior (2007) destaca que não houve medição completa entre tal construto e os outros dois (facilidade de uso e utilidade percebida) e, portanto, não o destaca como tão relevante no modelo. Alguns questionamentos para testar este construto são: Eu acho que seria importante utilizar o sistema em vez de usar o método atual? Seria muito melhor utilizar o sistema em vez do método atual?

A **intenção comportamental** é entendida como o grau em que uma pessoa tem intenção de desempenhar determinado comportamento. Alguns estudos a colocam como função direta da utilidade percebida sem considerar o construto atitude. Para testar este construto pode-se utilizar perguntas do tipo: dado que tenha acesso ao sistema, eu prevejo que o utilizaria?

Dias, Zwicker e Vicentin (2003) destacam como limitações do Modelo TAM a impossibilidade de analisar o contexto organizacional e avaliar apenas um sistema específico e não opções de sistemas distintas, mas suportam que tal modelo pode ser utilizado como importante ferramenta gerencial nas organizações. Já Rodrigues e Costa (2006) alertam que são os indivíduos que atuam e modificam as práticas, reforçando a importância de estudá-los juntamente com o modelo. Uma utilidade prática do modelo TAM foi apresentada por Silva e Dias (2006), na qual gerentes se utilizaram de tal modelo para ampliar um de seus construtos, a utilidade percebida.

Niño (2009, p. 42) faz breve relato dos modelos acima, destacando a comparação entre os modelos considerados como mais testados:

> Diversos autores fazem uma comparação conceitual entre TRA, TPB e TAM, levantando-se as diferenças e similaridades existentes entre os modelos. Nos três casos, observa-se a similaridade na proposta de que a atitude é determinada pelas crenças mais relevantes do indivíduo. Entretanto, o modelo TAM assume que crenças a respeito de utilidade percebida e facilidade de uso percebida são sempre os principais determinantes de decisões de uso de uma nova tecnologia. Já os modelos TRA e TPB assumem que cada para situação há crenças específicas envolvidas, que podem ser válidas em um determinado contexto e não em outro. Isto quer dizer que, para cada estudo utilizando os modelos TRA e TPB, é pertinente um levantamento preliminar das variáveis relevantes em determinado contexto, assim como quais são grupos de referência para usuários e quais são as crenças existentes em relação à determinada tecnologia. Resumindo, o TAM trata-se de um modelo mais específico,

> para avaliar o comportamento com relação à aceitação de tecnologia, enquanto a TRA e TPB são modelos bastante genéricos. Como consequência disso, Davis *et al* (1989) ressaltam que, enquanto no modelo TAM as variáveis específicas (crenças) são mais estáveis dentro do objetivo do modelo, nos outros modelos estas são redefinidas a cada contexto por se tratarem de modelos genéricos demais.

Outros modelos foram propostos como adaptações do Modelo TAM, como o modelo Chau de 1996 e Leaderer *et al*. de 2000. Eles consistem em detalhar algum construto ou incluir um novo, mas a base permanece a mesma que é a verificação de fatores que interferem na adoção de tecnologias.

Também baseado no Modelo TAM e nas Teorias TRA e TPB, Almeida e Sobral (2005) propuseram o Modelo Organizacional de Atitudes perante a Tecnologia da Informação (MOATI) que é apresentado no diagrama 7.

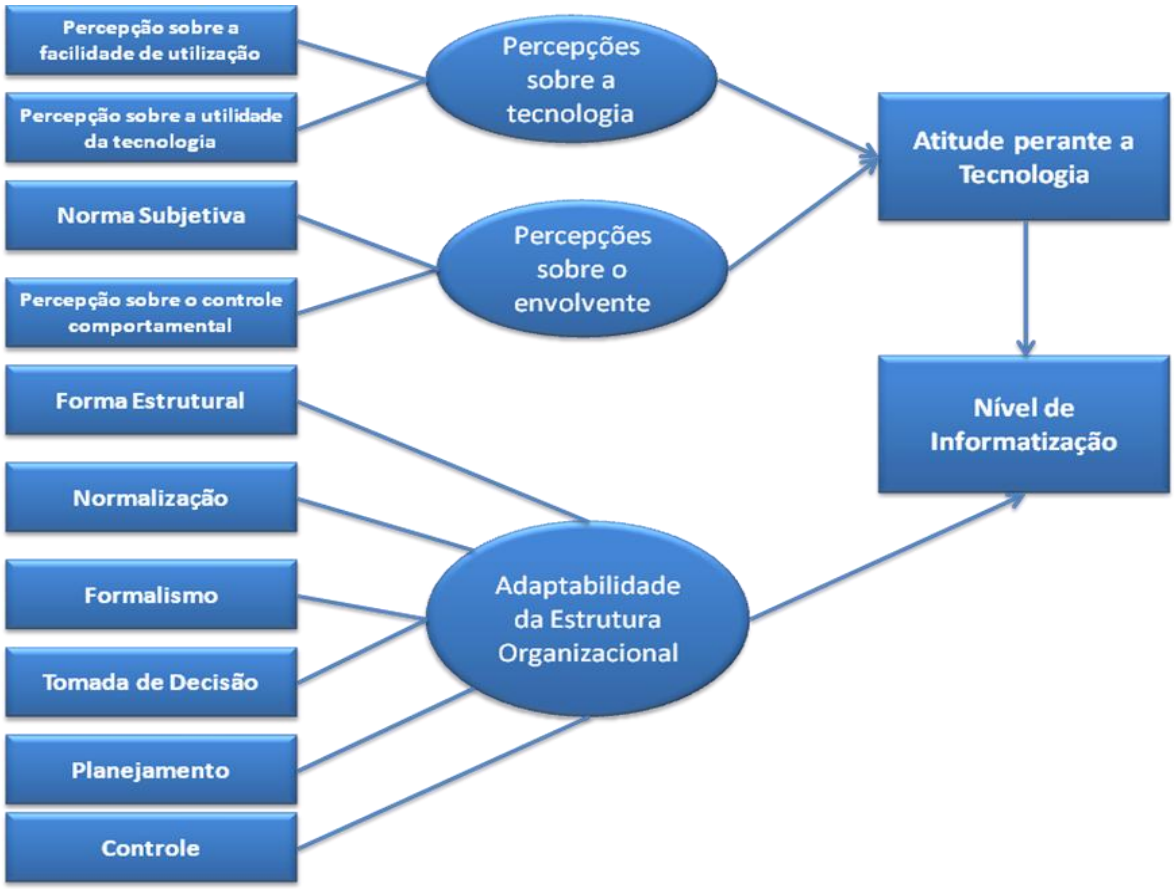


Diagrama 7. Modelo de Atitudes perante a tecnologia e informatização (MOATI)
Fonte: Almeida e Sobral (2005)

Este modelo inclui ao TAM variáveis relacionadas ao processo estrutural da organização que influenciam na tomada de decisão (ALMEIDA; SOBRAL, 2005). Ele é particularmente adaptado ao dirigente empresarial. Além disso, são analisadas as questões relativas ao meio onde a organização está inserida como a norma subjetiva e a percepção sobre o controle comportamental.

O Modelo MOATI se utiliza de contribuições incorporadas da TPB e TRA, além dos construtos do próprio modelo TAM. O diferencial deste modelo em relação às demais variações do TAM é que ele considera uma perspectiva de adaptação do ambiente organizacional, levando em conta a adaptação a mudanças.

Segundo Almeida e Sobral (2005), o Modelo MOATI representa um esforço teórico de combinação de variáveis individuais e organizacionais não relacionadas com a estratégia ou negócio da empresa, que poderão influenciar significativamente a informatização.

Venkatesh e Davis (2000) propuseram uma versão mais complexa do modelo original, o TAM2 que acrescenta outras variáveis aos modelos e possibilita análises mais detalhadas dos fatores que influenciam na aceitação e adoção de tecnologias, conforme diagrama 8.

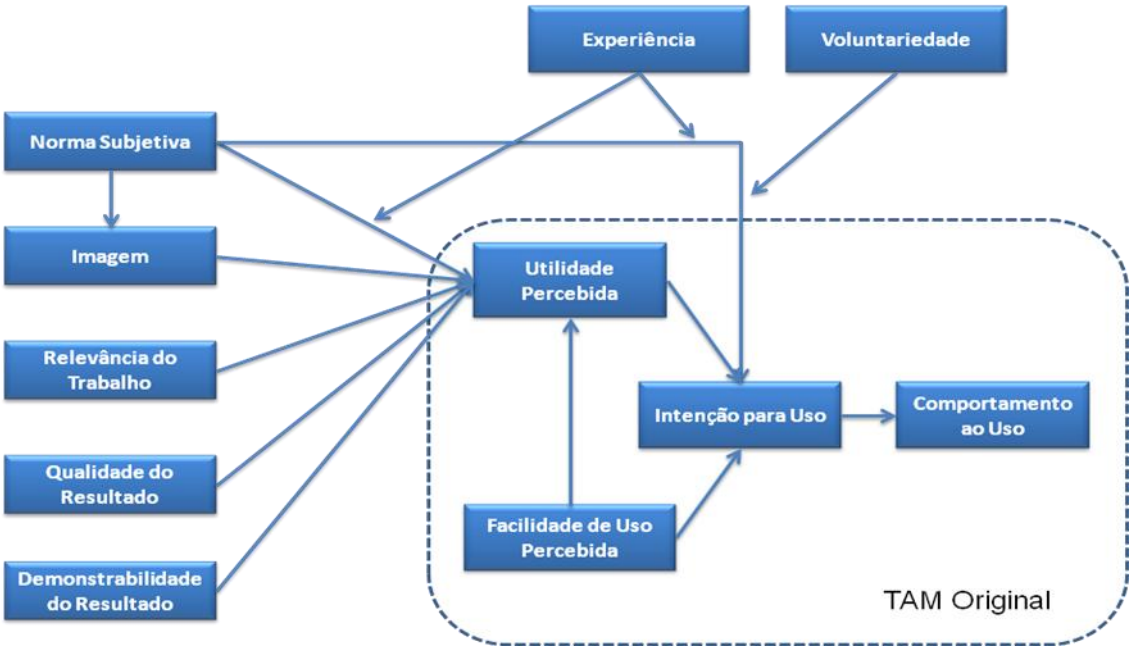


Diagrama 8. Relação dos construtos do modelo TAM2
Fonte: VEKANTESH (2009)

O modelo TAM2 testa outros relacionamentos. No caso da utilidade percebida, pode-se verificar sua influência por variáveis como: norma subjetiva, imagem, relevância do trabalho, qualidade do resultado e demonstrabilidade do resultado.

A norma subjetiva oriunda do TRA é utilizada como impulsionador da intenção de uso, já presente no modelo TAM original, porém sofrendo influência da voluntariedade. Desta relação pode-se extrair que as normas subjetivas são relevantes em situação de uso obrigatório, mas não de uso voluntário.

Desta forma a experiência e voluntariedade são consideradas como fatores que podem afetar a intenção de uso, sendo que o primeiro também pode afetar a utilidade percebida. Neste caso, o pesquisador pode verificar se o tempo de serviço em uma organização tem relação direta com o construto utilidade percebida e a intenção em usar tecnologias. E se o fato da pessoa ter um perfil voluntário afeta sua intenção da utilização de tecnologias. Tais testes são muitos importantes para direcionar a adoção de ações para públicos específicos.

Niño (2009, p. 48) resume o TAM2 da seguinte forma:

> O modelo TAM2 sugeriu que processos de influência social (norma subjetiva, voluntarismo e imagem) e processos instrumentais cognitivos (relevâncias de trabalho, qualidade de produção, demonstrabilidade de resultado e facilidade de uso percebida) são variáveis determinantes sobre a utilidade percebida e as intenções de uso. Assim mesmo, os autores do modelo identificaram uma diminuição na força com que os processos de influência sociais afetam a utilidade percebida e a intenção de uso com o passar do tempo e com a experiência crescente do indivíduo.

Venkatesk (2009) ainda apresenta um modelo criado por ele em 2003 em conjunto com outros três autores, dentre eles Davis, o criador do Modelo TAM original. A criação do modelo, denominado UTAUT, ou Teoria Unificada do Uso da Aceitação e Uso de Tecnologia, tem como principal intenção a unificação de modelos e teorias relacionados à aceitação de tecnologias. Tal autor ainda descreve um modelo mais recente o TAM3 criado por ele e Bala em 2008, no qual tais autores acrescentam algumas variáveis como influenciadores da Facilidade de Uso Percebida. A definição dos construtos do Modelo TAM3 apresentado por Venkatesk (2009) consta no quadro 8.

CONSTRUTO	DEFINIÇÃO
Atitude	Sentimento positivo ou negativo sobre o desempenho do comportamento-alvo (por exemplo, utilização de um sistema).
Autoeficácia em ambiente tecnológico	Grau em que um indivíduo acredita que possui capacidade de executar tarefas específicas / trabalho utilizando computador.
Ansiedade computacional	Grau em que um indivíduo sente apreensão, ou mesmo medo, quando é confrontado com a possibilidade de utilização de computadores.
Diversão em ambiente tecnológico	Grau de espontaneidade cognitivo em interações com o computador.
Demonstrabilidade do Resultado	Tangibilidade dos resultados da utilização da inovação.
Experiência	Grau de facilidade associadas ao uso do sistema.
Prazer percebido	Medida em que a atividade de utilizar um sistema específico é percebida como agradável, independente de quaisquer consequências resultantes do desempenho sistema usar.
Imagem	Grau em que a utilização de uma inovação é percebida como um reforço do status social.
Intenção de Uso	Grau em que uma pessoa tem consciência e formula planos para executar ou não executar algumas especificado comportamento futuro.
Norma Subjetiva	Percepção de que a maioria das pessoas que são importantes para ele acha que ele deve ou não realizar o comportamento em questão.
Percepção de controle	Grau em que um indivíduo acredita numa infraestrutura técnica e organizacional existente de apoio à utilização do sistema.
Relevância do Trabalho	Percepção do indivíduo em relação ao grau em que o sistema alvo é relevante para o seu trabalho.
Saída de qualidade	Grau em que um indivíduo acredita que o sistema executa o seu trabalho bem tarefas.
Usabilidade Objetiva	Comparação de sistemas baseados no nível real (ao invés de percepções), do esforço necessário para completar tarefas específicas.
Utilidade Percebida	Grau em que um indivíduo acredita que a utilização do sistema irá ajudá-lo a atingir ganhos de desempenho profissional.
Voluntariedade	Medida em que os potenciais adotantes percebem a adoção como decisão não-obrigatória.

Quadro 8. Definição dos construtos do modelo TAM 3
Fonte: Vekantesh (2009)

Da análise Modelo TAM3 proposto por Venkatesh e Bala em 2008, percebe-se que os construtos ampliados a partir do TAM2 interferem especialmente na Facilidade de Uso Percebida. Tais construtos são classificados em dois tipos, a saber: de fundamento ou base (ansiedade computacional, autoeficácia em ambiente tecnológico, percepção de controle e diversão em ambiente tecnológico) e os de sistematização (Usabilidade Objetiva e Prazer Percebido).

3. METODOLOGIA

Este capítulo descreve os aspectos da metodologia de pesquisa, através de detalhamento de sua classificação metodológica, população e amostra da pesquisa, método e instrumento de coleta de dados, modelo de pesquisa e operacionalização das variáveis.

Apesar de não ser exigida pela norma a separação destes tópicos em subseções, adotou-se esta prática por fins didáticos.

3.1CLASSIFICAÇÕES METODOLÓGICA DA PESQUISA

O trabalho analisou os fatores que influenciam gestores públicos estaduais nas suas percepções em relação à aceitação de práticas avançadas de Gestão da Segurança da Informação. Assim, do ponto de vista de seus objetivos, a pesquisa é classificada como **descritiva** uma vez que ela descreveu um fenômeno ou situação, mediante um estudo realizado em determinado espaço-tempo (MARCONI; LAKATOS, 1999).

Em relação à forma de abordagem, a pesquisa é **quantitativa**, pois as opiniões e informações foram traduzidas em números que, em seguida, classificados para análises através de recursos e de técnicas estatísticas. Os métodos quantitativos são empregados em pesquisas de âmbito social, econômico, de comunicação, mercadológicas, de opinião, de administração, representando em linhas gerais, uma forma de garantir a precisão dos resultados, e, evitando com isso, distorções de análise e interpretações. (OLIVEIRA; 1997).

3.2 POPULAÇÃO E AMOSTRA DA PESQUISA

A Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação (ABEP) é composta por organizações responsáveis pela Gestão de TI nos governos estaduais. Já as coordenações estaduais do Programa Nacional de Apoio à

Modernização da Gestão e do Planejamento dos Estados e do Distrito Federal (PNAGE) são formadas por gestores públicos responsáveis pelas ações mais atuais nas áreas transversais do governo (planejamento e gestão). Diante disso, tais gestores foram considerados como relevantes para descrever as ações do governo que representam.

Segundo Marconi e Lakatos (1999) o universo ou população é o conjunto de seres animados ou inanimados que apresentam pelo menos uma característica em comum. Como se pretende conhecer que fatores influenciam gestores públicos estaduais nas suas percepções em relação à aceitação de práticas avançadas de Gestão da Segurança da Informação, então, nesta pesquisa, o universo considerado é formado por dois tipos de gestores públicos: os considerados gestores de organizações especialistas em TI, que são os diretores estaduais das organizações filiadas à ABEP, e os gestores da área pública em geral (especialidade: planejamento e gestão), que são os coordenadores estaduais do PNAGE.

A motivação de escolha destes dois grupos para descrever a percepção de gestores públicos dos governos estaduais frente às práticas avançadas de TI justifica-se pelo fato de que por suas características específicas de trabalho, eles estão aptos a prestar informações coerentes sobre a situação atual de adoção de políticas de Segurança da Informação, uma vez que atuam na área como gestores ou usuários de nível tático e estratégico. O quantitativo da população foco da pesquisa é detalhado na tabela 1.

Tabela 1. Quantitativo detalhado da população.

UF	QUANTIDADE DA POPULAÇÃO	
	COORDENADORES DO PNAGE	DIRETORES DAS FILIADAS À ABEP
AC	04	04
AL	04	05
AM	04	03
AP	04	05
BA	04	05
CE	04	04
DF	04	0
ES	03	03
GO	0	02
MA	04	05
MG	04	06
MS	02	03
MT	01	04
PA	03	05
PB	05	03
PE	03	03
PI	04	03

PR	03	05
RJ	04	07
RN	03	04
RO	04	0
RR	04	04
RS	05	04
SC	04	04
SE	05	03
SP	04	05
TO	04	01
TOTAL	97	100

Fonte: Próprio autor (2008)

Para a análise se utilizou dados primários provenientes dos respondentes da pesquisa. A intenção inicial era realizar uma pesquisa censitária, pois buscou respostas de todos os Diretores das Organizações filiadas à ABEP e da totalidade dos Coordenadores do PNAGE. No entanto, como não houve resposta da totalidade dos respondentes, a estratégia foi alterada.

Hair *et al*. (2005) defende que não se deve realizar uma análise fatorial com uma amostra com menos de cinquenta observações. Como para o público de gestores de organizações especialistas em TI (Diretores das organizações filiadas à ABEP) houve apenas trinta e sete observações (quantitativo de respondentes) de um total de 100 (quantitativo da população), optou-se pelo descarte de tais questionários na análise.

Já para o público de gestores de organizações não especialistas em TI (Coordenadores do PNAGE) houve um número de respostas superior e as ausências são resultados de transição de equipe e outros eventos desta natureza, então se pode considerar como amostragem não aleatória por conveniência. De um total de noventa e sete pesquisados (quantitativo da população), houve resposta de oitenta (quantitativo da amostra).

3.3 MÉTODO DA PESQUISA E INSTRUMENTO DA COLETA DE DADOS

Para realização do estudo e coleta dos dados e informações foi utilizada a **pesquisa de campo**. Marconi e Lakatos (1999) descrevem que a pesquisa de campo é aquela

utilizada com o objetivo de conseguir informações e/ou conhecimentos acerca de um problema para o qual se procura uma resposta, ou de uma hipótese que se queira comprovar, ou, ainda, descobrir novos fenômenos ou, as relações entre eles. Ela consiste na observação de fatos e fenômenos tal como ocorrem espontaneamente, na coleta de dados a eles referentes e no registro de variáveis que se presumem relevantes, para analisá-los.

Nesta pesquisa, o instrumento de coleta de dados foi o **questionário**, que é um meio para obter respostas a questões de forma que o próprio informante o preencha. Tal instrumento de coleta é composto principalmente de itens estruturados (GOODE; HATT, 1977). Os questionários utilizados nesta pesquisa encontram-se nos Apêndices A e B.

Após construção da primeira versão do instrumento foram realizados pré-testes em agosto de 2008 com gestores públicos do Governo do Estado do Rio Grande do Norte. Algumas questões sobre a identificação do Respondente e da Organização causaram dificuldade de resposta por interpretação diversa, então elas foram ajustadas de forma a ficar mais claras.

Para os Coordenadores do PNAGE, gestores de planejamento e gestão, houve a realidade de coleta de dados conforme apresentado na tabela 2.

Tabela 2. Distribuição e devolução dos questionários do PNAGE

	DISTRIBUIÇÃO		**DEVOLUÇÃO**	
FORMA	**QUANTIDADE**	**%**	**QUANTIDADE**	**%**
Pessoalmente	48	49,5	41	51,3
Por terceiros	41	42,3	0	0
Por e-mail	8	8,2	27	33,7
Por fax	0	0	12	15
Pelo Correio convencional	0	0	0	0
TOTAL	**97**	**100**	**80**	**100**

Fonte: Próprio autor (2009)

Da tabela 2 se extrai que a forma de entrega predominante foi pessoalmente. Ela ocorreu da cidade de Recife, em Pernambuco, no mês de setembro de 2008, por ocasião da reunião trimestral do Colegiado Técnico Consultivo do PNAGE, onde se reuniram os Coordenadores do referido projeto para discutir suas ações. A segunda forma de distribuição mais relevante foi através de terceiros, uma vez que para os Estados que não contavam com todos os seus representantes no referido encontro, os questionários foram enviados por algum

representante da equipe estadual. Foi realizado um controle de entrega a terceiros conforme modelo no Apêndice C, para reduzir o risco de extravios. Para os poucos Estados que não estavam presentes no evento, os questionários foram enviados por e-mail.

Já em relação à devolução dos questionários preenchidos pelos respondentes, verifica-se que a forma predominante permanece sendo pessoalmente, uma vez que quase todos que receberam desta forma, devolveram os questionários preenchidos durante o mesmo evento no qual receberam tais instrumentos. Os demais respondentes enviaram por e-mail e como última opção, por fax. Não houve devolução de questionário por terceiros ou pelo correio convencional.

Como limitação da coleta de dados, resultando em dezessete questionários não devolvidos, verifica-se a rotatividade das equipes e ausência por férias ou viagens de trabalho de membros da equipe do PNAGE no período da pesquisa. Apesar disto, a estratégia adotada apresentou-se como bem sucedida, uma vez que a quantidade de questionários não devolvidos pode ser considerada baixa. O período de coleta dos questionários do PNAGE estendeu-se de setembro de 2008 a janeiro de 2009.

Em relação aos Diretores das organizações filiadas à ABEP, gestores de organizações especialistas em TI, houve a realidade de coleta de dados apresentada na tabela 3.

Tabela 3. Distribuição e devolução dos questionários da ABEP

	DISTRIBUIÇÃO		**DEVOLUÇÃO**	
FORMA	**QUANTIDADE**	**%**	**QUANTIDADE**	**%**
Pessoalmente	5	5	5	14,3
Por terceiros	95	95	3	8,6
Por e-mail	0	0	17	42,9
Por fax	0	0	9	25,7
Pelo Correio convencional	0	0	3	8,5
TOTAL	**100**	**100**	**37**	**100**

Fonte: Próprio autor (2009)

Da tabela 3 se extrai que a forma de entrega predominante dos Diretores das organizações filiadas à ABEP foi através de terceiros, uma vez que houve impossibilidade da pesquisadora participar de evento nacional que concentrava a maioria dos respondentes. Foi realizado um controle de entrega a terceiros conforme modelo no Apêndice D para reduzir o

risco de extravios. Os Coordenadores do PNAGE foram os portadores dos questionários e eles deveriam entregar aos Diretores das Organizações Filiadas à ABEP e providenciar seu envio para a pesquisadora. Para os poucos Estados onde houve contato pessoal, a distribuição foi feita desta forma.

Já em relação à devolução dos questionários preenchidos pelos respondentes, verifica-se que predominância da forma por e-mail seguida do envio por fax. Também houve devolução pelo correio convencional, pessoalmente e por terceiros.

Como limitação da coleta de dados, resultando em sessenta e quatro questionários não devolvidos, verifica-se os seguintes itens: a) impossibilidade de entrega dos questionários pessoalmente aos respondentes; b) interpretação de que deveria ser respondido apenas um questionário por Estado; c) possibilidade de dificuldade nas respostas. Esta última limitação se deve ao fato de que a pesquisadora considerou que os gestores das organizações filiadas à ABEP fossem especialistas em TI e, pelas respostas obtidas nos trinta e sete questionários, verificou-se apenas conhecimentos básicos nesta área. Diante disso, pode-se questionar se os que não responderam, não o fizeram pelo pouco conhecimento na área.

O período de coleta dos questionários dos Diretores das organizações filiadas à ABEP estendeu-se de outubro de 2008 a abril de 2009 e contou com apoio da Secretária da ABEP que enviou e-mail aos Diretores no primeiro trimestre de 2009, solicitando aos que não tinham respondido o questionário, que o fizessem e enviassem para o e-mail da pesquisadora.

Uma questão verificada entre a devolução dos dois tipos de questionários é que o do PNAGE obteve resposta de representantes de todos os Estados pesquisados (25 Estados e o Distrito Federal), enquanto para os da ABEP, dos 25 Estados com representação, apenas representantes das filiadas à ABEP em treze deles responderam, ou seja, quase 50% dos Estados pesquisados.

3.4 OPERACIONALIZAÇÃO DAS VARIÁVEIS

As variáveis utilizadas na pesquisa são de dois tipos. As **variáveis independentes**, conforme a seguir:

Percepção sobre a facilidade de uso de práticas de Segurança. Construto

elaborado a partir do Modelo TAM. As perguntas do questionário foram utilizadas para verificação desta variável encontram-se elaboradas através de escala Likert em cinco níveis de gradação, desde o “discordo totalmente” até o “concordo totalmente”.

Percepção sobre a utilidade de práticas de Segurança. Construto elaborado a partir do Modelo TAM. As perguntas do questionário foram utilizadas para verificação desta variável encontram-se elaboradas através de escala Likert em cinco níveis de gradação, desde o “discordo totalmente” até o “concordo totalmente”

Perfil demográfico dos gestores públicos. Construto elaborado para caracterizar os respondentes. As perguntas do questionário foram utilizadas para verificação desta variável encontram-se elaboradas através de escala de múltipla escolha com resposta única, escala de categoria simples (dicotômica) ou resposta livre.

Perfil comportamental dos gestores públicos. Construto elaborado com base em teorias comportamentais como a TRA que foi utilizada como base de desenvolvimento do modelo TAM. As perguntas do questionário foram utilizadas para verificação desta variável encontram-se elaboradas através de escala de múltipla escolha com resposta única.

Perfil organizacional do uso da TI. Construto elaborado para caracterizar os respondentes. As perguntas do questionário foram utilizadas para verificação desta variável encontram-se elaboradas através de escala de múltipla escolha com resposta única ou resposta livre.

Atitude perante as práticas de Segurança. Construto elaborado a partir do Modelo TAM. As perguntas do questionário foram utilizadas para verificação desta variável encontram-se elaboradas através de escala Likert em cinco níveis de gradação, desde o “discordo totalmente” até o “concordo totalmente”.

Intenção de utilização das práticas de Segurança da Informação. Construto elaborado a partir do Modelo TAM. As perguntas do questionário foram utilizadas para verificação desta variável encontram-se elaboradas através de escala Likert em cinco níveis de gradação, desde o “altamente improvável” até o “altamente provável”.

A **variável dependente** é verificada através do nível de aceitação quanto às práticas avançadas de gestão de Segurança da Informação. Para a medição de atitudes e opiniões há inúmeros tipos de escalas. Por meio das técnicas escalares pode-se transformar uma série de fatos qualitativos em uma série de fatos quantitativos ou variáveis, podendo-se aplicar processos de mensuração e de análise estatística (MARCONI; LAKATOS, 1999).

Nesta pesquisa foram utilizados dois tipos de questionário com escala Likert, sendo que, para os respondentes de organizações especialistas em TI, diretores das empresas

filiadas à ABEP, adotou-se tal escala nas opções (1) não implantado, (2) em análise, (3) em implantação, (4) implantado parcialmente, (5) implantado e disseminado. Além destes, conta o nível 0 foi utilizado como escala de implantação e serve apenas como opção de desconhecimento da resposta pelo gestor. Pelo baixo índice de resposta, este tipo de questionário foi descartado na fase de análise.

Já para os respondentes do PNAGE, a escala variou entre as opções (1) discordo totalmente, (2) discordo, (3) não concordo, nem discordo, (4) concordo e (5) concordo totalmente.

A primeira etapa de análise dos resultados utilizou técnicas análise descritiva visando atingir os três primeiros objetivos específicos desta pesquisa de descrição do perfil dos respondentes e da organização.

Em seguida, utilizou-se técnicas de análise fatorial onde as assertivas que medem a aceitação dos pesquisados em relação às práticas da Norma ISO/IEC 27001 foram reduzidas a cinco fatores. Tais assertivas encontram-se na parte IV do Questionário e representam recomendações da referida norma nos domínios de “Controle de Acesso” e “Recursos Humanos”. Tais domínios foram escolhidos por serem de mais fácil compreensão por ambos os públicos respondentes (de TI e de gestão/planejamento) e por tratarem questões que geralmente são implementadas de forma preliminar, sendo, portanto, na maioria dos casos, precursoras das demais.

A análise conclui com a regressão múltipla onde se testou a significância de relacionamentos entre as variáveis independentes com cada um dois fatores, objetivando testar as hipóteses da pesquisa. A pesquisa adotou nível de significância de 5%, o que significa que as decisões feitas em relação aos testes são realizadas ao nível de 95% de confiança. Tais técnicas foram escolhidas por seu forte alinhamento com os objetivos da pesquisa, permitindo a realização de todos os testes desejados.

3.5 MODELO DA PESQUISA

O modelo adotado nesta pesquisa baseia-se no Modelo TAM e sua representação é detalhada no diagrama 9.

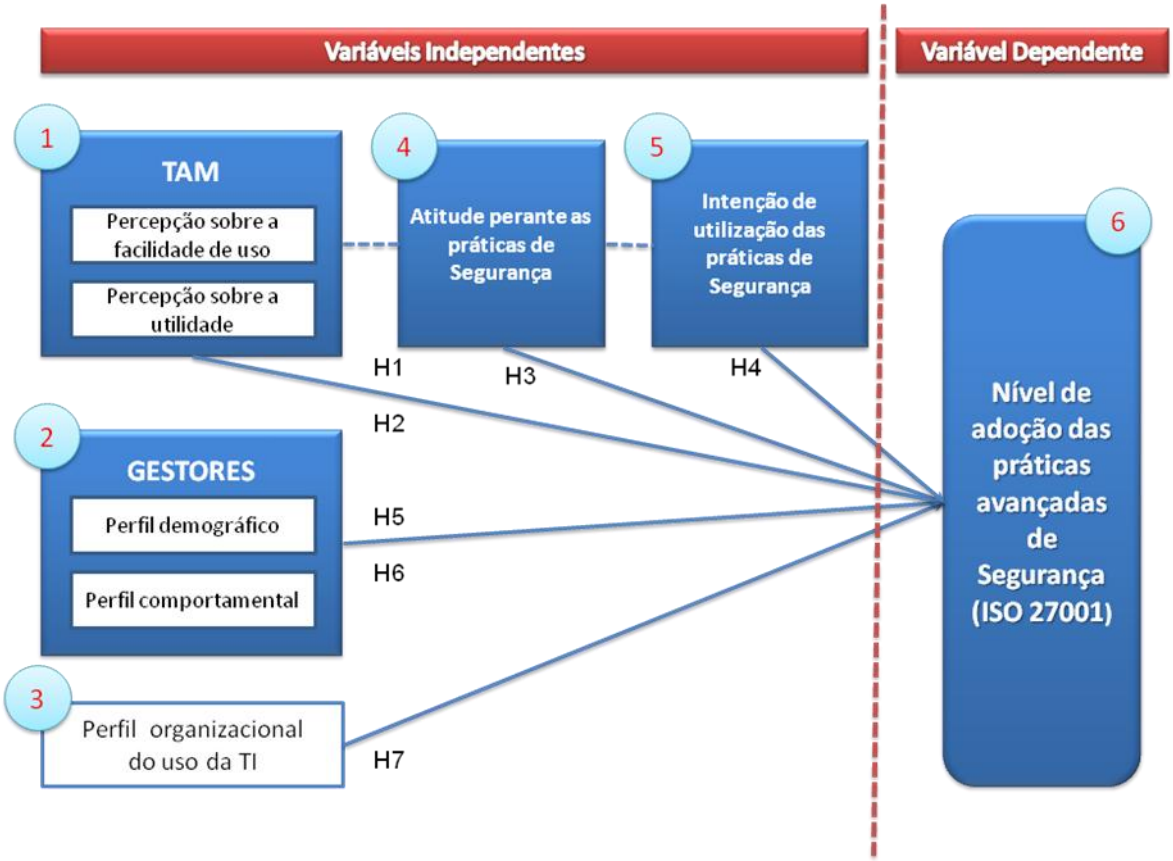


Diagrama 9. Modelo teórico da pesquisa
Fonte: Próprio autor (2008)

Tal modelo é uma adaptação do Modelo de Aceitação de Tecnologia (TAM), desenvolvido por Davis em 1986 e, é utilizado como modelo teórico desta pesquisa. As seguintes hipóteses são representadas no diagrama 9 através da letra H:

H1) As percepções sobre a facilidade de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança;

H2) As percepções sobre a utilidade de práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança;

H3) As percepções sobre a atitude perante as práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança;

H4) A intenção de utilização das práticas de Segurança exerce uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança;

H5) O perfil demográfico dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança;

H6) O perfil comportamental dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança;

H7) O perfil organizacional exerce influência significativa perante a adoção de práticas avançadas de Segurança.

As hipóteses representadas na figura pela letra "H" consistem do relacionamento entre variáveis independentes com a variável dependente de nível de adoção na norma. As variáveis representadas pelos números 1, 4 e 5 são provenientes do Modelo TAM. As variáveis 2 e 3 são provenientes de teorias comportamentais e utilizadas para categorizar os respondentes da pesquisa e a variável dependente (número 6) representa o nível de adoção que será gerado através de análise fatorial das assertivas da Norma ISO 27001:2005 constantes na parte IV do instrumento de pesquisa.

O quadro 9 apresenta a correspondência entre as hipóteses, as variáveis testadas no modelo e as respectivas perguntas do instrumento de pesquisa que as testam.

HIPÓTESE	VARIÁVEIS	PERGUNTAS DO QUESTIONÁRIO
H1	1(a) e 6	18 e 19
H2	1(b) e 6	20 e 21
H3	4 e 6	22 e 23
H4	5 e 6	24 e 25
H5	2(a) e 6	9 a 15
H6	2(b) e 6	16 e 17
H7	3 e 6	1 a 8

Quadro 9. Correspondência entre modelo, hipóteses e questionário
Fonte: Próprio autor (2008)

No quadro 9, verifica-se que todas as hipóteses podem ser testadas a partir de perguntas no questionário que relacionam sempre uma variável independente com a variável independente gerada a partir das assertivas na norma ISO 27001.

4. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

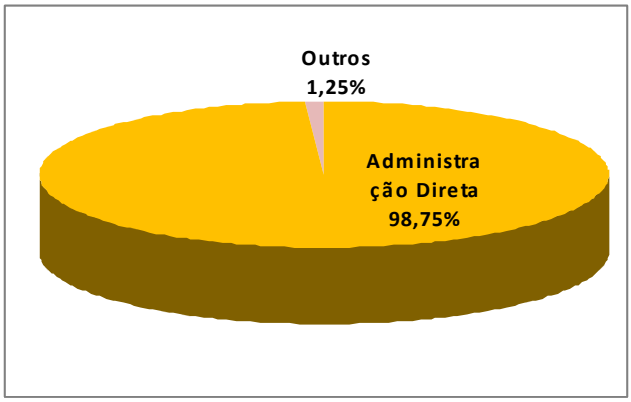
Este capítulo é dividido em quatro partes, sendo a primeira relativa à estatística descritiva que é utilizada para caracterizar os respondentes, através da descrição do perfil organizacional, demográfico e comportamental da amostra. A segunda parte é onde constam os resultados da análise fatorial que reduz as respostas às assertivas da norma ISO 27001 (parte IV do questionário) em fatores. Na terceira parte são apresentados os resultados da análise de regressão múltipla e na parte final é apresentada a validação das hipóteses.

4.1 ESTATÍSTICA DESCRITIVA

Com vistas a atingir os objetivos da pesquisa, o trabalho de análise se inicia com a descrição da organização e dos respondentes. Para a descrição do perfil demográfico dos gestores utilizam-se dois tipos de análise. Em relação às variáveis categóricas é realizada a análise de percentual. Todas as tabelas relacionadas aos gráficos apresentados em tal análise encontram-se nos apêndices F, G e H. Já para variáveis quantitativas são utilizadas técnicas de estatística descritiva como valor mínimo, valor máximo, média e desvio padrão.

A primeira parte do questionário trata de caracterizar o perfil organizacional. Assim, analisando-se o gráfico 1 nota-se que 98,75% dos entrevistados estão em organizações da Administrativa Direta e 1,25% de outros tipos de organização. Isso demonstra forte alinhamento e dependência das decisões organizacionais com as políticas definidas pelo Governo do Estado e infere-se redução de autonomia nas decisões.

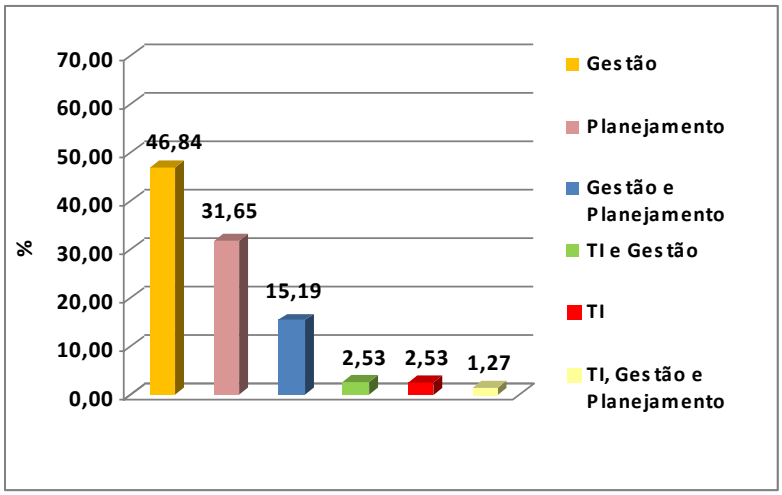
Gráfico 1 – Distribuição de frequências do tipo da organização



Fonte: Resultados da pesquisa (2009)

A variável "setor de atuação da organização" é demonstrada através do gráfico 2 e nele nota-se que 46,84% das organizações dos respondentes são do setor de gestão, 31,65% são de planejamento, 15,19% no setor de Gestão e Planejamento e apenas uma pequena quantidade atua em outras áreas (6,63%). Tal resposta já era esperada, uma vez que os respondentes são coordenadores do PNAGE e tal projeto está intrinsecamente vinculado às Secretarias Estaduais de Planejamento e Gestão.

Gráfico 2 – Distribuição de frequências do setor de atuação

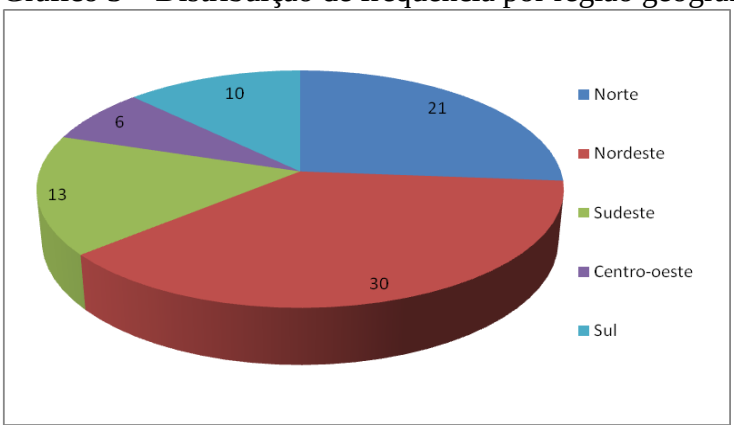


Fonte: Resultados da pesquisa (2009)

O Gráfico 3 apresenta o quantitativo de gestores por região geográfica do Brasil. A região Nordeste conta com 30 respondentes da pesquisa, seguida pela Região Norte com 21 e das regiões sudeste, sul e centro-oeste que somam 13, 10 e 6 respondentes

respectivamente. Como a quantidade de respondentes por Estado é praticamente fixa, pois existem, normalmente, três coordenadores do PNAGE por Estado, percebe-se que a variação do quantitativo de respondentes por região se dá em função das regiões com um maior número de Estados.

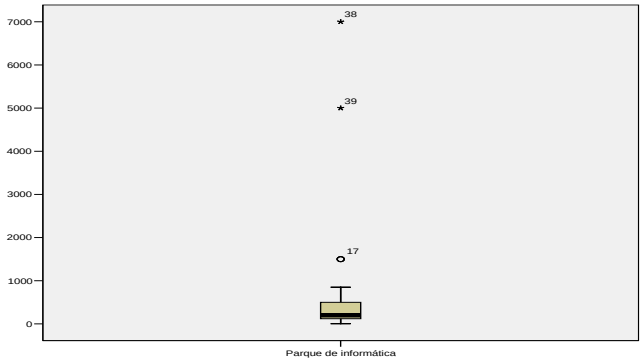
Gráfico 3 – Distribuição de frequência por região geográfica



Fonte: Resultados da pesquisa (2009)

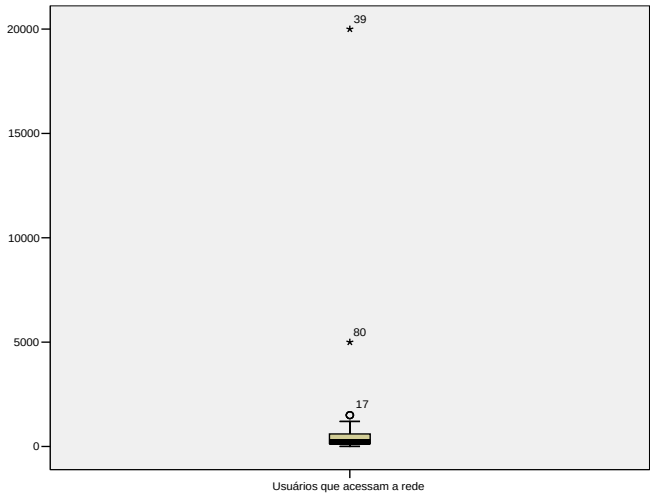
Ainda em relação à primeira parte do questionário que buscou descrever o padrão organizacional no uso da TI, utilizou-se de perguntas com variáveis quantitativas que são analisadas pelas técnicas de estatística descritiva como valor mínimo, valor máximo, média e desvio padrão a análise de percentual. Em relação ao parque de informática e usuários que acessam a rede de informática verifica-se nos gráficos de dispersão 4 (parque de informática) e 5 (usuários que acessam a rede) que há uma variabilidade muito alta das respostas. Os gráficos de dispersão foram adotados para ilustrar a variabilidade das respostas.

Gráfico 4 – Dispersão do parque de informática



Fonte: Resultados da pesquisa (2009)

Gráfico 5 – Dispersão de usuários da rede



Fonte: Resultados da pesquisa (2009)

A Tabela 4 apresenta as duas variáveis quantitativas (parque de informática e usuários da rede). Antes de formatar a referida tabela foram retiradas as ocorrências onde as variáveis eram iguais a zero, isto porque foi dada ao respondente a opção zero se houvesse desconhecimento da resposta. Com a retirada das ocorrências onde houve resposta zero, resultam em quarenta e duas variáveis em relação a **usuários da rede** e quarenta e cinco variáveis de **parque de informática**.

Tabela 4. Estatística descritiva do perfil organizacional

Variável	Mínimo	Máxima	Média	Desvio padrão
Parque de informática	4	850	246,05	211,68
Usuários que acessam a rede	4	900	264,34	223,719

Fonte: Resultados da pesquisa (2009)

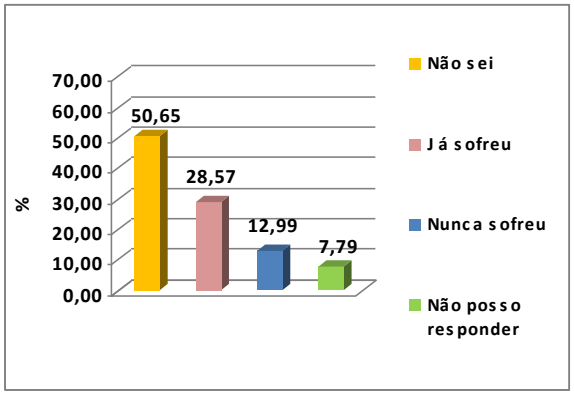
Em relação ao parque de informática além das respostas zeradas, também foram descartadas outras sete ocorrências (posições 17 a 19, 24, 38 a 39 e 80), cujos valores são: 1.200, 1.500, 5.000 e 20.000 porque eles representam erro na compreensão da questão. A mesma ação para usuários que acessam a rede resultou no descarte de sete observações de sete ocorrências (posições 17 a 19, 38 a 40 e 80), cujos valores são: 1.500, 5.000 e 7.000 e também representam erro de interpretação.

Mesmo com tais descartes, ainda se percebe uma variação muito alta, onde nota-se que alguns responderam em relação à rede de informática de todo o Governo

Estadual, outros em relação a sua unidade de trabalho (setor dentro da organização) e outros em relação a toda a organização. Diante disto, a análise deste item fica prejudicada.

Através do Gráfico 6, nota-se que 50,65% dos entrevistados não sabe se a organização onde trabalham já sofreu alguma incidência de ataques, 28,57% afirmaram que já sofreram, 12,99% declararam nunca sofreram e 7,79% dos entrevistados afirmaram que não poderia responder. O índice alto no desconhecimento de ataques pode demonstrar falta de interesse pelas questões de segurança da informação ou até mesmo pouca disseminação de tais assuntos na organização.

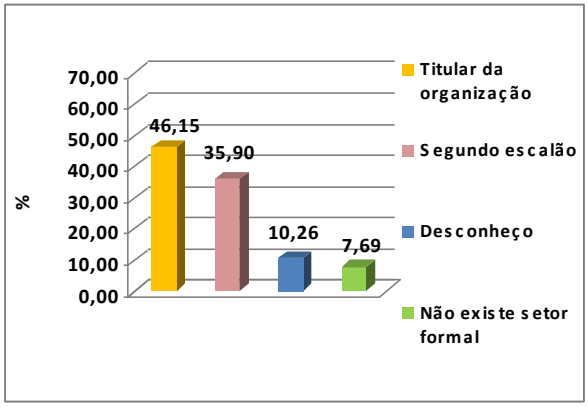
Gráfico 6 – Distribuição de frequências de Incidência de ataque



Fonte: Resultados da pesquisa (2009)

O Gráfico 7 mostra que 46,15% dos entrevistados afirmaram que o setor responsável pela segurança é vinculado diretamente ao titular da organização. 35,90% declararam que é ao segundo escalão, 10,26% afirmaram que desconhecem e 7,69% informaram não existir setor formal. Um índice significativo (quase metade dos respondentes – 46,15%) informou que o setor responsável pela segurança da informação é vinculado diretamente ao titular da organização, o que pode demonstrar maior autonomia.

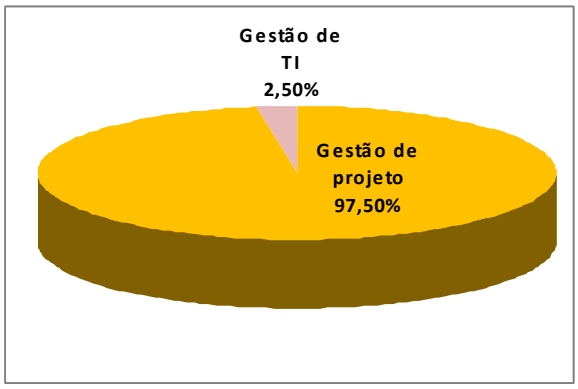
Gráfico 7 – Distribuição de frequências da Hierarquia do Setor de SI



Fonte: Resultados da pesquisa (2009)

Em relação à segunda parte do questionário, tem-se a caracterização do perfil dos respondentes. Em relação à área de atuação dos respondentes, percebe-se ampla maioria (97,50%) na área de gestão de projetos e apenas uma pequena parte (2,50%) na área de gestão de TI, conforme ilustrado no gráfico 8. Tal resultado já era esperado, uma vez que o público especialista em TI (diretores das organizações filiadas à ABEP) teve que ser descartado pelo pequeno índice de respostas.

Gráfico 8 – Distribuição de frequências de área de atuação



Fonte: Resultados da pesquisa (2009)

Na tabela 5, verifica-se uma média de idade dos respondentes de pouco mais de quarenta e três anos de idade. O desvio padrão pode ser considerado relativamente alto, apresenta uma dispersão dos dados em relação a média de aproximadamente 10 anos, atingindo um percentual de variação de vinte e por cento da média. Tal resultado já era esperado uma vez que se trata de uma pesquisa nacional onde os governos estaduais estão em

estágios diferentes no seu tratamento em relação às políticas públicas de Recursos Humanos para provimento da tabela funcional. Assim, entende-se que, nos Estados onde há uma maior rotação de pessoal com contratação de novos servidores efetivos ou apenas comissionados, a média de idade esperada é mais baixa, no entanto, naquele onde há maior dificuldade de renovação da tabela por escassez de concursos públicos para a área de gestão a média de idade deve ser alta, favorecendo uma média já esperada, com desvio padrão relativamente alto.

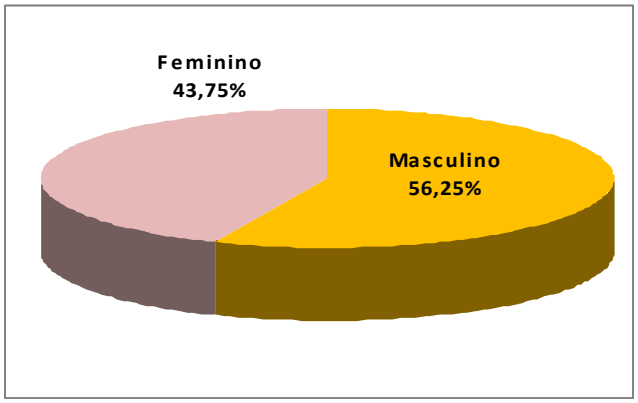
Tabela 5. Idade dos respondentes

Variável	Mínimo	Máxima	Média	Desvio padrão
Idade	25	60	43,18	10,09

Fonte: Resultados da pesquisa (2009)

Em relação ao sexo dos respondentes, percebe-se um equilíbrio com pequena maioria para o público masculino que totaliza 56,25% enquanto o feminino é de 43,75% conforme ilustrado no gráfico 9.

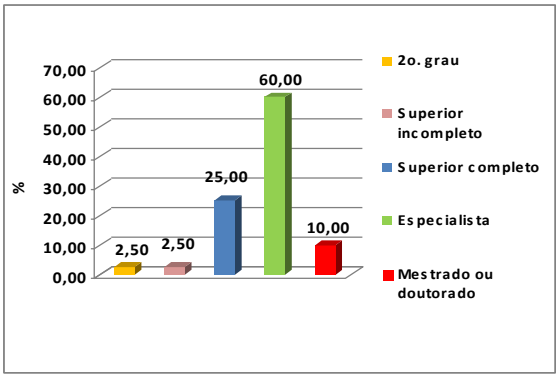
Gráfico 9. Distribuição do sexo dos respondentes



Fonte: Resultados da pesquisa (2009)

O nível de escolaridade é relativamente alto conforme demonstra gráfico 10, sendo que oitenta e cinco por cento possuem nível superior completo ou acima deste e conta com 70% com nível de pós-graduação. Tal resultado não surpreende, uma vez que tais gestores atuam na definição de políticas públicas dos governos de seus estados e precisam constantemente se articular com organismos de outras esferas de governos e até internacionais, o que carece de maior nível de conhecimento.

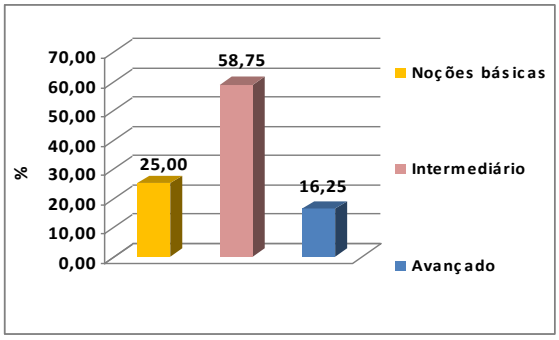
Gráfico 10 – Distribuição de frequências do nível de escolaridade



Fonte: Resultados da pesquisa (2009)

O nível de conhecimento em informática foi outra variável pesquisada para descrever o perfil demográfico do respondente, uma vez que a pesquisa relaciona-se ao tema. Para esta variável percebe-se que a maioria dos respondentes (58,75%) possui nível intermediário de conhecimento, como demonstrado no gráfico 11. Considerando que tais gestores não são, na sua maioria, gestores de organizações especialistas em TI e sim em projetos, o resultado pode ser considerado de acordo com as expectativas.

Gráfico 11 – Distribuição de frequências de conhecimento geral em informática

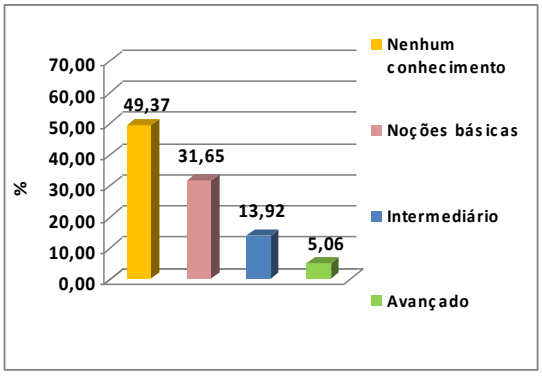


Fonte: Resultados da pesquisa (2009)

Como forma de verificar o equilíbrio entre as respostas sobre o nível de conhecimento em TI, onde a maioria dos respondentes informou ter conhecimento intermediário conforme demonstrado no gráfico 11, perguntou-se também sobre a frequência de treinamento em rede e segurança da informação. A expectativa era de que a maioria permanecesse no nível básico nesta pergunta, uma vez que pode se considerar que quem tem algum conhecimento em TI também tenha feito alguma capacitação em conceitos de

segurança da informação e/ou rede de computadores, no entanto, o que demonstra o gráfico 12 é que a maioria (49,37%) informou que não possui nenhum conhecimento na área, seguida por 31,65% que disse ter noções básicas. Isso nos leva a considerar que a maioria dos respondentes possui conhecimentos na área de TI apenas como autodidata e que não deve existir preocupação nas organizações onde trabalham de capacitação de seus servidores em relação às precauções sobre práticas de segurança da informação.

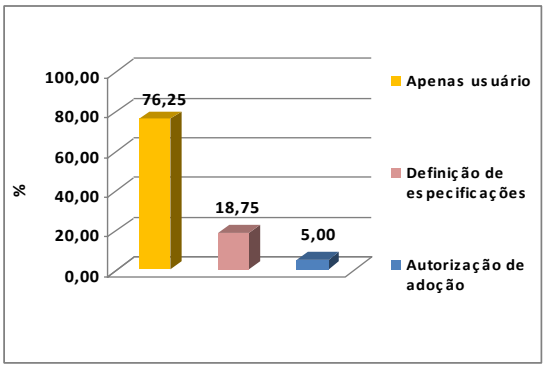
Gráfico 12 – Distribuição de frequências de treinamento em rede e/ou segurança da informação



Fonte: Resultados da pesquisa (2009)

Para verificar o poder de decisão do gestor na adoção de tecnologia, perguntou-se se ele apenas adota as novas tecnologias impostas pela organização, se ele é quem define ou se ele autoriza tais aquisições. Como se percebe no gráfico 13, a maioria (76,25%) é de apenas usuários que não possuem nenhuma interferência na escolha ou autorização de novas tecnologias.

Gráfico 13 – Distribuição de frequências do papel na adoção de novas tecnologias

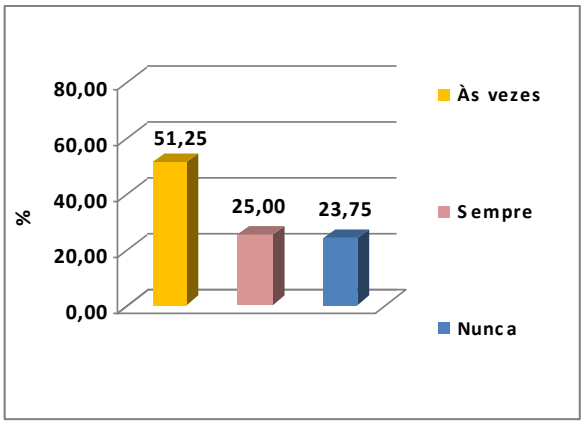


Fonte: Resultados da pesquisa (2009)

Com a descrição das respostas obtidas nas variáveis: idade, área de atuação, sexo, nível de escolaridade, nível de conhecimento de TI, nível de capacitação em rede e/ou segurança da informação e papel na adoção de novas tecnologias, espera-se ter atingido o objetivo específico desta pesquisa de descrição demográfica dos respondentes. O segundo objetivo específico que trata do perfil comportamental dos gestores públicos pode ser atingido verificando-se o quão ousado o respondente é em relação aos riscos que corre na área de segurança da informação, conforme gráficos 14 e 15 e, também nas respostas em relação aos construtos do modelo TAM, que serão vistos na sequência.

O gráfico 14 demonstra que quase um quarto dos respondentes (23,75%) não usa nunca e exatamente um quarto (25%) a utiliza sempre, ficando o restante, que é a maioria (51,25%) na situação de utilização eventual.

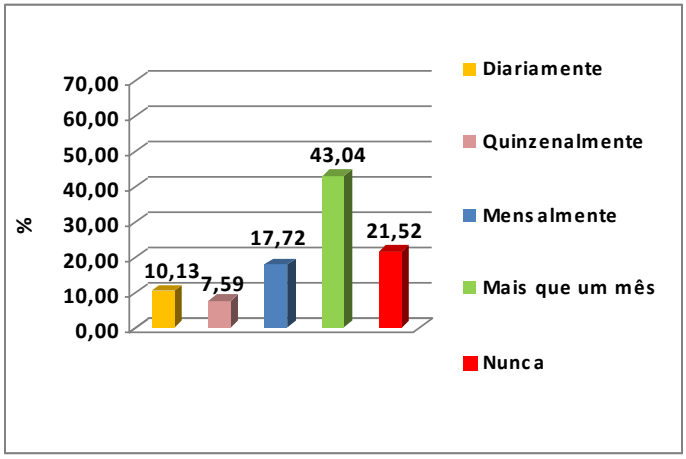
Gráfico 14 – Distribuição de frequências do uso de rede do trabalho para acessar contas pessoais



Fonte: Resultados da pesquisa (2009)

Já o gráfico 15 ilustra a frequência de realização de backups de arquivos realizados pelos respondentes. A maioria (43,04%) respondeu que faz mais que um por mês, no entanto, uma parcela considerável de quase um quatro dos respondentes (21,52%) disse que não faz nunca demonstrado uma grande quantidade de respondentes sem preocupações com questões relacionadas a segurança da informação nas suas práticas cotidianas. Embora não se tenha verificado na pesquisa se as organizações em que trabalham realizam backup corporativo, esta pergunta foi adotada para avaliar o grau de preocupação dos usuários com planos de contingência.

Gráfico 15 – Distribuição de frequências das vezes que costuma fazer back up de seus arquivos

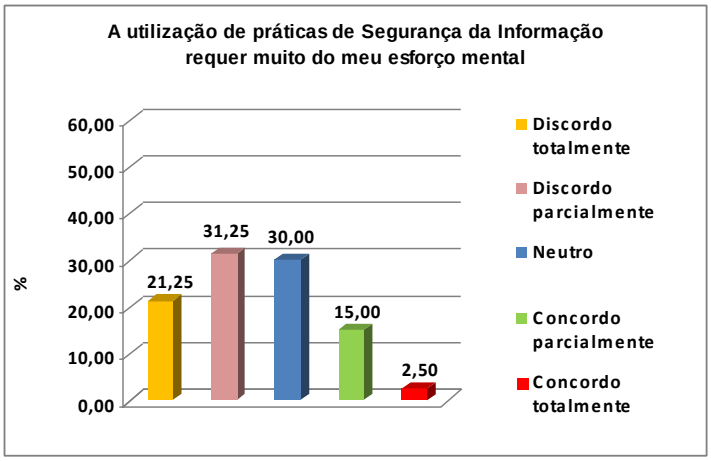


Fonte: Resultados da pesquisa (2009)

A parte três do questionário contém oito questões que testam a concordância e possibilidade de adoção dos respondentes em relação às práticas avançadas de segurança da informação. Tais questões são típicas do Modelo TAM e as respostas obtidas são descritas conforme a seguir.

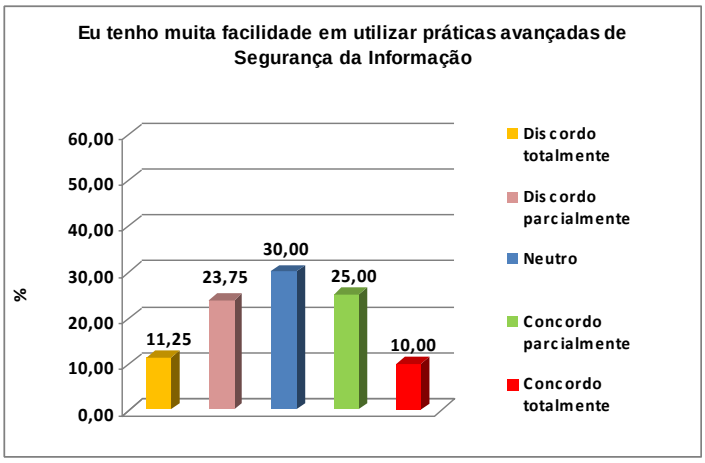
A **Facilidade de Utilização** das práticas de Segurança que será utilizada para testar a hipótese 1 é verificada nas perguntas 18 e 19 do questionário e suas respostas constam dos gráficos 16 e 17.

Gráfico 16 – Respostas modelo TAM - facilidade de utilização 1



Fonte: Resultados da pesquisa (2009)

Gráfico 17 - Respostas modelo TAM - facilidade de utilização 2

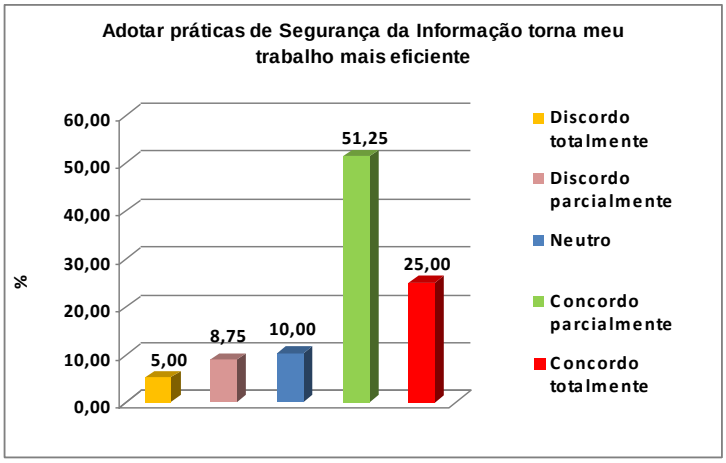


Fonte: Resultados da pesquisa (2009)

Da análise das respostas à pergunta "**A utilização de práticas de Segurança da Informação requer muito do meu esforço mental**", ilustrada pelo gráfico 16, verifica-se que um percentual significativo permaneceu neutro em ambas as questões (30%) e que 52,5% discorda de que a utilização de práticas requer muito esforço mental, no entanto, na análise das respostas à pergunta "**Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação**", apresentada no gráfico 17, apenas 35% alegou ter muita facilidade na adoção de tais práticas.

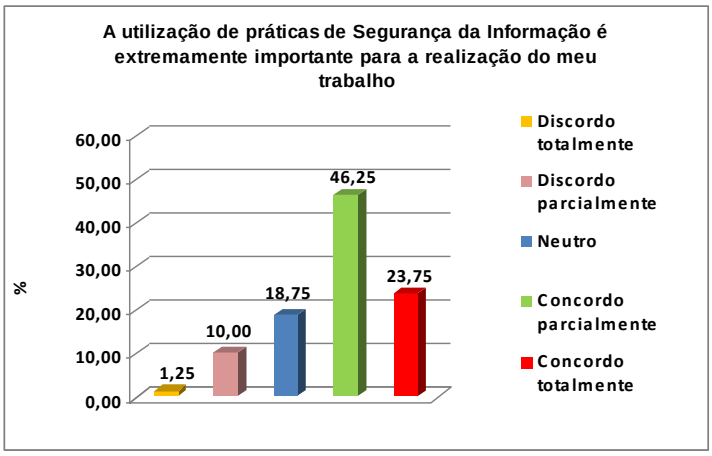
As **Percepções sobre a Utilidade** de Práticas de Segurança é outra variável do Modelo TAM. Ela é verificada pelas perguntas 20 e 21 do questionário e seus resultados são apresentados nos gráficos 18 e 19.

Gráfico 18 - Respostas modelo TAM – percepções sobre a utilidade 1



Fonte: Resultados da pesquisa (2009)

Gráfico 19 - Respostas modelo TAM – percepções sobre a utilidade 2

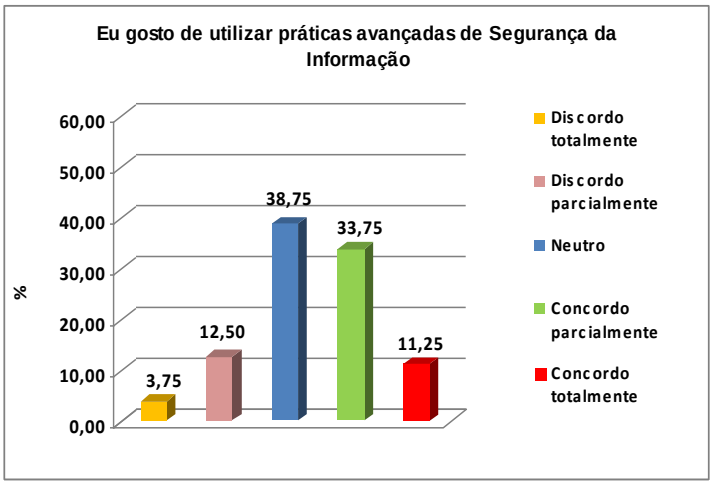


Fonte: Resultados da pesquisa (2009)

Da análise das respostas à pergunta "**Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente**", ilustrada pelo gráfico 18, verifica-se que o nível de concordância foi acima de 75%. Já da análise das respostas à pergunta "**A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho**", apresentada no gráfico 19, o nível de concordância é de 70%. Ambos os resultados apresentam índice bastante significativo para esta variável do Modelo TAM em termos de aceitação dos respondentes.

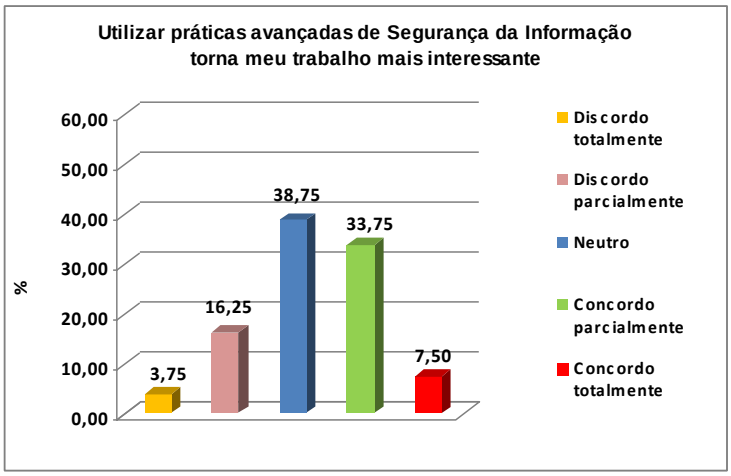
As Percepções sobre a **Atitude** perante as Práticas de Segurança é outra variável do Modelo TAM. Ela é verificada pelas perguntas 22 e 23 do questionário e seus resultados são apresentados nos gráficos 20 e 21.

Gráfico 20 - Respostas modelo TAM – atitude 1



Fonte: Resultados da pesquisa (2009)

Gráfico 21 - Respostas modelo TAM – atitude 2

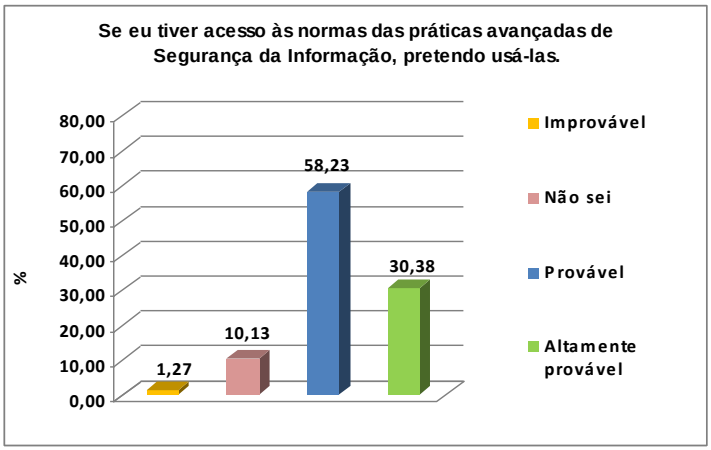


Fonte: Resultados da pesquisa (2009)

Em ambas as questões ligadas à atitude o índice de neutro foi bastante significativo (38,75%). Da análise das respostas à pergunta "**Eu gosto de utilizar práticas avançadas de Segurança da Informação**", ilustrada pelo gráfico 20, verifica-se que a maioria dos demais respondentes (excluindo-se os neutros) optou pela concordância (45%). Já da análise das respostas à pergunta "**Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante**" (gráfico 21) também mais de 40% optaram pela concordância.

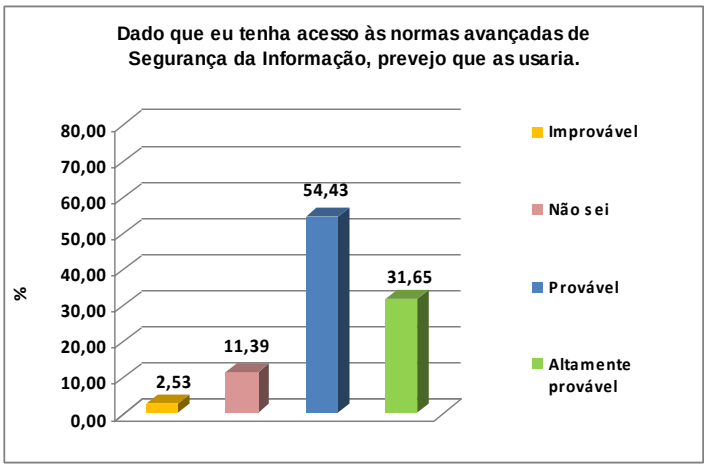
As Percepções sobre a **Intenção de Utilização** de Práticas de Segurança é outra variável do Modelo TAM. Ela é verificada pelas perguntas 24 e 25 do questionário e seus resultados são apresentados nos gráficos 22 e 23.

Gráfico 22 - Respostas modelo TAM – intenção de utilização 1



Fonte: Resultados da pesquisa (2009)

Gráfico 23 - Respostas modelo TAM – intenção de utilização 2



Fonte: Resultados da pesquisa (2009)

Da análise das respostas à pergunta "**Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-la**", ilustrada pelo gráfico 22, verifica-se que a maioria dos demais respondentes optou pela concordância (30,38% de altamente provável e 58,23% de provável). Já da análise das respostas à pergunta "**Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria**" (gráfico 23), quase 32% optaram pela concordância, através da seleção de resposta "altamente provável" e mais de 54% adotaram a resposta "provável".

4.2 ANÁLISE FATORIAL

Com objetivos de atingir os dois últimos objetivos da pesquisa ("Aferir a percepção de aceitação dos gestores públicos quanto às práticas avançadas em Gestão de Segurança da Informação, em conformidade com as diretrizes da Norma ISO 27001" e "Verificar as associações existentes entre o perfil dos gestores públicos, perfil organizacional e a aceitação de Normas Avançadas de Gestão de Segurança da Informação") foram utilizadas duas técnicas de estatística: a análise fatorial e a regressão linear múltipla.

A análise Fatorial (AF) é uma técnica que busca, através da avaliação conjunta de variáveis, a identificação de dimensões de variabilidade comuns existentes em um conjunto de fenômenos; o intuito é desvendar estruturas existentes, mas que não são observáveis diretamente. Cada uma dessas dimensões de variabilidade comum recebe o nome de FATOR

(CORRAR; PAULO; DIAS FILHO, 2007). Em outras palavras, a AF tem como objetivo apresentar um conjunto de variáveis originais através da criação de um número menor de dimensões ou Fatores.

Neste estudo, existem 20 variáveis dependentes originais que compõem a Adoção de Práticas Avançadas de Segurança da Informação em conformidade com a Norma ISO 27001. Tais perguntas estão organizadas da seguinte forma: da pergunta 1 a 14 e mais a pergunta 20 (de V1 a V14 + V20) se referem ao domínio de Controle de Acesso e da pergunta 15 a 19 (de V15 a V19) correspondem ao domínio de Recursos Humanos.

O objetivo da utilização da AF é reduzir este conjunto de variáveis a um número menor de variáveis compostas (Fatores) para uso em análise multivariada subseqüente (Regressão Linear Múltipla). Um Fator nada mais é do que uma combinação linear das variáveis originais. Cada Fator deve ser interpretado como uma dimensão ou Fator da adoção de praticas avançadas de segurança.

Os resultados obtidos através da análise fatorial, verificados através da matriz de correlação (constante no Apêndice I deste trabalho) demonstram baixo índice de correlação entre as variáveis originais (diversos índices abaixo de 0,40). Na parte inferior da mesma tabela verifica-se a significância (sig. Ou p-test). Para se obter uma boa AF, os valores devem ser próximos a zero. Neste caso, na grande maioria os p-valores foram baixos.

Além da matriz de correlação, observou-se outro teste que nos permite avaliar se os dados originais viabilizam a utilização da AF de forma satisfatória. O teste de *Kaiser-Meyer-Olkin* (*Measure of Sampling Adequacy* – MAS) indica o grau de explicação dos dados a partir dos Fatores encontrados na AF.

Caso o MSA indique um grau de explicação menor que 0,50, significa que os Fatores encontrados na AF não conseguem descrever satisfatoriamente as variações dos dados originais. Através da tabela 6 verifica-se que o teste indicou um alto poder de explicação entre os Fatores e as variáveis (0,8279).

Tabela 6 - KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,827885
Bartlett's Test of Sphericity	Approx. Chi-Square	656,3867
	DF	190
	Sig.	0,0000

Fonte: Resultados da pesquisa (2009)

Outro teste que pode ser visualizado na mesma tabela é o teste de esfericidade de Bartlett que indica se existe relação suficiente entre as variáveis para aplicação da AF. Para que seja possível a aplicação da AF, recomenda-se que o valor de Sig. (teste de significância) não ultrapasse 0,05. Caso isso ocorra, é provável que a correlação das variáveis seja muito pequena, o que impede a aplicação da AF. Nota-se que o teste indica a possibilidade de aplicação do AF nas variáveis analisadas (0,000).

A matriz anti-imagem (constante no Apêndice I deste trabalho) indica o poder de explicação dos Fatores em cada uma das variáveis analisadas. A diagonal da parte inferior da mesma tabela indica o MSA para cada uma das variáveis analisadas. Esses valores encontram-se na diagonal principal. Os valores inferiores a 0,50 são considerados muito pequenos para análise e nesses casos indicam variáveis que podem ser retiradas da análise. Segundo esse critério, nenhuma das variáveis de Adoção de práticas avançadas de Segurança deve ser retirada, pois todos os MAS estão acima de 0,50.

A maioria das variáveis conseguiu um poder de explicação alto, considerando todos os Fatores obtidos na análise de comunalidades (constante no Apêndice I deste trabalho). Alguns Fatores obtiveram explicações razoáveis (abaixo de 0,70).

Uma última análise que pode ser feita antes de se realizarem outros testes é o grau de explicação atingido pelos 5 Fatores que foram calculados pela AF. Com relação a esse indicativo, apesar da fraca relação entre os Fatores e algumas variáveis, o modelo consegue explicar 63% da variância dos dados originais, o que é uma percentual considerável. É possível observar isso na tabela Total de Variância Explicada (constante no Apêndice I deste trabalho).

Dessa forma, acredita-se ter chegado a um grau de relacionamento e explicação das variáveis capaz de ser útil na avaliação da Adoção de praticas avançadas de Segurança. A Tabela 7 (*Component Matrix*) permite verificar qual dos Fatores melhor explica cada uma das variáveis consideradas.

Tabela 7 – *Component Matrix*

	Component				
Variável	**1**	**2**	**3**	**4**	**5**
V1	0,6424	-0,2981	-0,1872	-0,3944	0,1842
V2	0,4835	0,0152	0,1159	0,5641	0,3844
V3	0,5863	0,1495	-0,0973	-0,1748	-0,4975
V4	0,6965	-0,1070	0,0523	-0,3968	0,0024
V5	0,6616	0,0647	-0,0758	0,0287	-0,0960
V6	0,7145	0,2274	-0,0757	-0,0985	0,1196

V7	0,6086	0,2872	0,0039	0,0845	-0,0390
V8	0,4900	0,5567	-0,1949	-0,0532	0,0835
V9	0,5136	0,3695	0,3670	-0,1875	0,2200
V10	0,4576	0,6053	0,2008	0,1316	0,1793
V11	0,5314	-0,1314	0,2841	0,4488	-0,2107
V12	0,4029	-0,2745	-0,3597	0,0197	0,5202
V13	0,5339	-0,2867	0,5547	-0,3370	-0,0529
V14	0,6617	-0,2874	0,2391	0,0877	0,1619
V15	0,5688	-0,5497	-0,0353	0,3101	-0,1519
V16	0,5659	0,2148	-0,1525	0,1586	-0,3370
V17	0,7264	-0,0582	-0,3789	0,0840	-0,1791
V18	0,7242	-0,0713	-0,2911	0,0950	-0,0571
V19	0,5657	-0,1016	0,4492	0,0180	-0,0980
V20	0,7531	-0,1095	-0,1595	-0,1447	0,1050

Fonte: Resultados da pesquisa (2009)

A Tabela 7 permite uma classificação mais precisa das variáveis em cada um dos Fatores. O objetivo inicial de reduzir-se o número de variáveis da parte IV do questionário através da análise fatorial e facilitar a fase seguinte de análise resultou em cinco fatores, conforme quadro 10.

FATOR		ASSERTIVA NORMA	
1	Usuários	V1	Cada identificador de acesso da rede (ou login) deve ser único para cada usuário
		V3	Os usuários da rede devem se comprometer, por escrito, a manter sigilo de suas senhas
		V4	A reativação de senhas (para usuários que se esqueceram da senha) deve ser feita após identificação rigorosa de que é o próprio usuário quem está requerendo a reativação
		V5	Os direitos de acesso à rede devem ser revisados regularmente
		V6	Os usuários devem ser alertados a evitar registrar senhas em papel
		V7	Os usuários devem ser obrigados a alterar suas senhas em intervalos regulares de tempo
		V9	O procedimento de entrada na rede (ou login) deve ser limitado a três tentativas
		V11	Devem existir cuidados especiais para utilização de recursos de computação móvel (ex: notebooks)
		V14	Devem existir mecanismos de monitoramento/gravação de imagens das instalações físicas onde os equipamentos de controle da rede funcionam
		V15	Devem existir regras claras de responsabilização de má utilização dos recursos da rede
		V16	Deve existir alguma verificação do passado do pretenso usuário da rede para verificar se ele já infringiu alguma norma de segurança em empregos anteriores
		V17	Os novos usuários da rede devem assinar algum documento tomando ciência de suas responsabilidades para segurança das informações que utilizará no seu trabalho
		V18	Todos os usuários da rede devem receber treinamento adequado para as suas respectivas funções sobre suas responsabilidades na segurança das informações
		V19	Os usuários que cometem erros através de falhas de segurança devem ser formalmente responsabilizados através de processos disciplinares
		V20	Deve existir um procedimento formal para criação de um novo usuário na rede e registro de seu nível de acesso

2	Senhas	V8	A entrada de senhas deve ser efetuada através do uso do mouse (teclado virtual)
		V9	O procedimento de entrada na rede (ou login) deve ser limitado a três tentativas
		V10	O sistema de gerenciamento de senhas deve proibir reutilização de senhas
3	Biometria	V13	Deve existir controle de acesso físico por biometria na área de utilização da rede
4	Férias	V2	A rede não deve aceitar login de usuários que estão de férias
5	Desligamento	V12	Quando um usuário é desligado da organização, seus direitos de acesso devem ser imediatamente removidos

Quadro 10 – Fatores da pesquisa
Fonte: Próprio autor (2009).

Todas as assertivas da norma referentes ao domínio de Recursos Humanos (seção A8 da ISO 27001) foram agrupadas no fator 1.

4.3 ANÁLISE DE REGRESSÃO MÚLTIPLA

Depois de realizada a análise fatorial, é feita a regressão múltipla dos fatores com as variáveis explicativas. Cada Fator será chamado de variável dependente e as demais variáveis indicada no campo dos questionários serão explicativas. A análise de regressão linear múltipla exige que a escala de medida das variáveis sejam métricas. Nas circunstâncias que as variáveis sejam não métricas serão incluídas no modelo as denominadas variáveis *dummy*, isto é, criar categorias ditas **dicotômicas**. Uma variável dicotômica é aquela que representa uma categoria de uma variável independente não métrica. Qualquer variável não-métrica com k categoria pode ser representada por k – 1 variáveis dicotômicas. Por exemplo, **sexo** tem duas categorias, feminino e masculino. Para representar a variável não-métrica sexo, criam-se duas novas variáveis dicotômicas (X_1 e X_2), onde representaria os indivíduos do sexo masculino com um valor 1 e daria a todos os do sexo feminino o valor 0. Neste estudo, a V18 tem 5 categorias (escala de 1 a 5), definiu-se 4 variáveis dicotômicas (X_1 a X_4). E assim por diante, cada variável explicativa com k categorias transformou-se em k -1 categorias.

De acordo com Hair *et al.* (2005), a análise de regressão múltipla é uma técnica estatística que pode ser usada para analisar a relação entre uma única variável dependente e várias variáveis independentes, com o objetivo de usar as variáveis independentes, cujos valores são conhecidos, para estimar a variável dependente selecionada pelo pesquisador,

onde cada variável independente tem seu peso, que denota a sua contribuição relativa para a predição da variável dependente. O conjunto de variáveis independentes ponderadas forma a variável estatística regressão, uma combinação linear das variáveis independentes que melhor prevê a variável dependente.

No geral, o modelo de Regressão Linear Múltipla é representado pela expressão:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_k X_k + \varepsilon$$

onde os parâmetros β_j, j = 0, 1, 2, ..., k são chamados de coeficientes de regressão, Y representa a variável dependente e X_i, i =1, 2, ...,k as variáveis independentes. (MONTGOMERY; PECK, 1992).

Para compreender-se melhor este tipo de análise, é importante que alguns termos estatísticos sejam esclarecidos:

- ***Coeficiente de regressão*** **(b_j)** é valor numérico do parâmetro estimado diretamente associado com uma variável independente. Representa a quantidade de mudança na variável dependente para uma unidade de mudança na variável independente. No modelo de predição múltiplo, os coeficientes de regressão são coeficientes parciais porque cada um leva em consideração não apenas a relação entre a variável dependente e as vaiáveis independentes, mas também entre variáveis independentes. (HAIR *et al.*; 2005)
- ***Coeficiente de determinação*** **(R^2)** mede a proporção da variação da variável dependente sobre seu significado que é explicado pelas variáveis independentes, podendo variar entre 0 e 1.
- ***Análise de Variância*** **(ANOVA)** é técnica estatística para determinar se as variáveis independentes explicam uma variação significativa na variável dependente.

Para o presente estudo, a regressão múltipla foi realizada para cada um dos fatores em relação a cada uma das hipóteses. As seções seguintes detalham tais análises.

4.3.1 Análise de regressão múltipla para o fator 1-usuários

Para a **hipótese H1** (as percepções sobre a facilidade de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança) verifica-se o comportamento apresentado nas tabelas 8, 9 e 10 ao relacionar-se a **Facilidade de Uso** das Práticas de Segurança com o Fator 1-Usuários da pesquisa. Para esta pesquisa, considerou-se como facilidade de uso, as respostas dadas às perguntas 18 e 19 da parte III do questionário, ou seja: "V18 - A utilização de práticas de Segurança da Informação requer muito do meu esforço mental"; "V19 - Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação".

Tabela 8 - *Model Summary* do Fator 1 (variável dependente) com Facilidade de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,432	0,187	0,091	0,953

Fonte: Resultados da pesquisa (2009)

Tabela 9 – ANOVA do Fator 1 (variável dependente) com Facilidade de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	14,20	8,00	1,77	1,95	0,07
Residual	61,80	68,00	0,91		
Total	**76**	**76**			

Fonte: Resultados da pesquisa (2009)

Tabela 10 – *Coefficients* do Fator 1 (variável dependente) com Facilidade de Uso

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0,3436	0,3522		0,9754	0,3328
V18.2 (X1)	-0,7044	0,3090	-0,3320	-2,2796	0,0258
V18.3 (X2)	-0,8513	0,3177	-0,3922	-2,6794	0,0092
V18.4 (X3)	-1,0552	0,3879	-0,3570	-2,7200	0,0083
V18.5 (X4)	-0,0552	0,7371	-0,0088	-0,0749	0,9405
V19.2 (X5)	-0,0382	0,3984	-0,0163	-0,0959	0,9239
V19.3 (X6)	0,4200	0,3910	0,1935	1,0742	0,2865
V19.4 (X7)	0,5121	0,3972	0,2222	1,2893	0,2017
V19.5 (X8)	0,3373	0,4747	0,1036	0,7107	0,4797

Fonte: Resultados da pesquisa (2009)

A análise da tabela 10 nos fornece o coeficiente de correlação (R) de 0,432, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,187 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 1-Usuários) é explicado pelas variações na variável independente. Em nosso exemplo, 18,7% da variação no Fator 1 são explicados pelas variações nas variáveis explicativas (V18 e V19).

O teste do ANOVA é um teste para determinar se existe uma relação linear entre a variável de resposta y e um subconjunto de regressores X_1, X_2, ..., X_k. As hipóteses apropriadas são:

$$H_0 : \beta_1 = \beta_2 = ... = \beta_k = 0$$
$$H_1 : \beta_j \neq 0 \ \ para\, no\, mínimo\, um\ j$$

A rejeição de H_0 : $\beta_1 = \beta_2 = \cdots = \beta_k = 0$ implica que no mínimo um dos regressores X_1, X_2, ..., X_k contribui significativamente para o modelo. O critério de decisão consiste em rejeitar H_0 quando o valor de Sig for pequeno. E neste caso, temos fortes evidências que o modelo ajustado demonstra relacionamento linear entre a variável dependente e o conjunto de variáveis independentes.

A tabela 14 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para o relacionamento descrito no modelo apenas a variável V18, com exceção da sua categoria dicotômica X_4, foi significativa para compor o modelo. Com isso, o modelo de regressão estimado extraído é:

$$\hat{Y} = 0,7044X_1 - 0,8513X_2 - 1,0552X_3$$

O modelo de regressão estimado indica que a V18 (A utilização de práticas de Segurança da Informação requer muito do meu esforço mental) reduz o Fator 1, isto é, a variável V18 e o Fator 1-Usuários estão correlacionados negativamente. Nota-se que X_1 (discorda), em média, reduz o Fator 1 em 0,70, a X_2 (não concordo, nem discordo) reduz o Fator 1 em 0,85 e a X_3 (concordo) reduz em 1,05; já a X_4 (concordo totalmente) não

apresentou relação significativa com o Fator 1 (sig. Ou P = 0,9405). Isto é compreensível, pois V18 apresenta uma pergunta na qual sua resposta negativa representa concordância com a facilidade de uso, ou seja, quanto mais se discorda com o esforço mental requerido pela utilização de práticas de Segurança da Informação, maior é a facilidade de uso percebida. Assim, conclui-se que houve correlação significativa entre o fator 1-usuários e a facilidade de uso em relação a esta variável independente (V18).

Analisando a variável V19 (Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação) verifica-se que não existe relação significativa com o Fator 1-Usuários, ou seja, para respondentes com facilidade de utilização de práticas ou não, o nível de concordância com as assertivas da ISO 27001 não variou significativamente. Isto pode representar problemas de interpretação da pergunta associada ao Modelo TAM (V19) ou necessidade de ampliação de pesquisa por não ter havido correlação esperada no que se refere a esta variável independente (V19).

Depois de testar a hipótese 1, a regressão múltipla foi realizada para a hipótese H2 (As percepções sobre a utilidade de práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança). Assim, verifica-se o comportamento apresentado nas tabelas 11, 12 e 13 ao relacionar-se a **Utilidade Percebida** das Práticas de Segurança com o Fator 1-Usuários da pesquisa. Para esta pesquisa, considerou-se como utilidade percebida, as respostas dadas às perguntas 20 e 21 da parte III do questionário, ou seja: "V20 - Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente"; "V21 - A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho".

Tabela 11 - *Model Summary* do Fator 1 (variável dependente) com Utilidade Percebida

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,555	0,309	0,238	0,873

Fonte: Resultados da pesquisa (2009)

Tabela 12 – ANOVA do Fator 1 (variável dependente) com Utilidade Percebida

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	23,453	7,000	3,350	4,399	0,0004
Residual	52,547	69,000	0,762		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

Tabela 13 – *Coefficients* do Fator 1 (variável dependente) com Utilidade Percebida

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0,620	0,953		0,650	0,518
V20.2 (X1)	0,888	0,424	0,257	2,092	0,040
V20.3 (X2)	-1,226	0,384	-0,532	-3,192	0,002
V20.4 (X3)	-0,383	0,301	-0,193	-1,274	0,207
V20.5 (X4)	-0,375	0,953	-0,115	-0,393	0,695
V21.2 (X5)	-0,227	0,927	-0,090	-0,245	0,807
V21.3 (X6)	-0,415	0,922	-0,209	-0,450	0,654
V21.4 (X7)	0,357	0,954	0,149	0,374	0,709
V21.5 (X8)	0,620	0,953		0,650	0,518

Fonte: Resultados da pesquisa (2009)

A análise da tabela 13 nos fornece o coeficiente de correlação (R) de 0,555, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,309 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variável dependente (Fator 1-Usuários) é explicado pelas variações na variável independente. Em nosso exemplo, 30,9% da variação no Fator 1-Usuários são explicados pelas variações nas variáveis explicativas (V20 e V21). Os resultados da ANOVA (sig. 0,0004) indicam que há fortes evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes.

A tabela 13 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para o relacionamento descrito no modelo, apenas a variável V20 (Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente), com exceção das duas categorias dicotômicas X_3 e X_4, foi significativa para compor o modelo. Com isso, o modelo de regressão estimado extraído é.

$$\hat{Y} = 0{,}888X_1 - 1{,}226X_2$$

O modelo de regressão estimado indica que a categoria nem concordam e nem discordo influenciam de forma negativa. Nota-se que X_1 (concorda), em média, aumenta o Fator 1 em 0,88, e a X_2 (nem concorda e nem discorda), em média, reduz o Fator 1 em 1,226. Já as demais categorias não apresentaram relação significativa com o Fator 1 (sig. Ou P > 0,10). Tais resultados demonstram que as pessoas que concordam que a adoção de práticas

de Segurança da Informação torne o trabalho mais eficiente possuem maior possibilidade em adotar tais práticas, já as pessoas com indiferença na questão (nem concordam, nem discordam) apresentam resistências ou dificuldades em adotá-las, ou seja, tais usuários poderão requerer atuação específica do gestor que visa implantar tais práticas, uma vez que elas demonstram mais resistência até mesmo que os que discordam de que a adoção de práticas avançadas de Segurança da Informação torna o trabalho mais eficiente.

Já a variável V21 (A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho) não apresentou correlação significante com o modelo, o que pode apontar para necessidade de mais pesquisas.

Os resultados da regressão múltipla de fatores no teste da hipótese H3 (As percepções sobre a atitude perante as práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança) para o Fator 1-Usuários verifica-se conforme comportamento apresentado nos tabelas 14 e 15 ao relacionar-se a **Atitude** perante as Práticas de Segurança com o Fator 1-Usuários. Para esta pesquisa, considerou-se como Atitude, as respostas dadas às perguntas 22 e 23 da parte III do questionário, ou seja: "V22 - Eu gosto de utilizar práticas avançadas de Segurança da Informação"; "V23 - Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante".

Tabela 14 - *Model Summary* do Fator 1 (variável dependente) com Atitude

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,329	0,108	0,009	1,000

Fonte: Resultados da pesquisa (2009)

Tabela 15 – ANOVA do Fator 1 (variável dependente) com Atitude

	Sum of Squares	df	Mean Square	F	Sig.
Regression	7,651	7,000	1,093	1,094	0,378
Residual	62,950	63,000	0,999		
Total	70,601	70,000			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V22 (Eu gosto de utilizar práticas avançadas de Segurança da Informação) e V23

(Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante) demonstrem relacionamento entre os Fatores analisados. Isto é, o Fator 1-Usuários não está sendo influenciado pelas variáveis independentes (V22 e V23). Isto representa que pessoas com atitude positiva, negativa e neutra perante a adoção de práticas avançadas de Segurança da Informação serão influenciadas da mesma forma por políticas para adoção das referidas práticas. Tais resultados, por não terem apresentado resultados esperados, apontam para necessidade de ampliação de pesquisa em relação ao construto Atitude do Modelo TAM.

A regressão múltipla de fatores também foi aplicada para testar a hipótese H4 (A intenção de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança) para o Fator 1-Usuários, conforme comportamento apresentado nas tabelas 16 e 17, que foram geradas ao relacionar-se a **Intenção de Uso** das Práticas de Segurança com tal fator. Para esta pesquisa, considerou-se como Intenção de Uso, as respostas dadas às perguntas 24 e 25 da parte III do questionário, ou seja: "V24 - Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las"; "V25 - Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria".

Tabela 16 - *Model Summary* do Fator 1 (variável dependente) com Intenção de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,283	0,080	0,002	0,999

Fonte: Resultados da pesquisa (2009)

Tabela 17 – ANOVA do Fator 1 (variável dependente) com Intenção de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	6,106	6,000	1,018	1,019	0,420
Residual	69,894	70,000	0,998		
Total	76,000	76,000			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V24 (Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las) e V25 (Dado que eu tenha acesso às normas avançadas de

Segurança da Informação, prevejo que as usaria) demonstram relacionamento entre os Fatores analisados. Isto é, o Fator 1-Usuários não está sendo influenciados pelas variáveis independentes (V24 e V25). Isto representa que pessoas com intenção positiva, negativa e neutra perante a adoção de práticas avançadas de Segurança da Informação serão influenciadas da mesma forma por políticas para adoção das referidas práticas. Tais resultados, por não terem apresentado resultados esperados, apontam para necessidade de ampliação de pesquisa em relação ao construto Intenção do Modelo TAM.

A regressão múltipla também foi aplicada para testar a hipótese H5 (O perfil demográfico dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança) para o fator 1-Usuários. Assim, verifica-se o comportamento apresentado nas tabelas 18 e 19 ao relacionar-se o Perfil Demográfico dos Gestores Públicos com o Fator 1 da pesquisa. Para esta pesquisa, considerou-se como Perfil Demográfico, as respostas dadas às perguntas 9 a 15 da parte II do questionário que identificam características do respondente, como sexo, idade, nível de escolaridade, nível de conhecimento em informática, entre outras.

Tabela 18 - *Model Summary* do Fator 1 (variável dependente) com Perfil Demográfico

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,345	0,119	-0,016	0,9942

Fonte: Resultados da pesquisa (2009)

Tabela 19 – ANOVA do Fator 1 (variável dependente) com Perfil Demográfico

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	8,706	10	0,871	0,881	0,556
Residual	64,254	65	0,989		
Total	72,960	75			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis demográficas (V9 a V15) demonstram relacionamento entre o Fator 1-Usuários, isto é, o Fator 1 não está sendo influenciado pelas variáveis demográficas (V9 a V15). Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil demográfico dos respondentes, inclusive utilizando outras técnicas estatísticas.

Para testar a hipótese H6 (O perfil comportamental dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança) foi realizada análise de regressão do perfil comportamental dos gestores com o Fator 1-Usuários, conforme resultado exposto nas tabelas 20 e 21. Para esta pesquisa, considerou-se como Perfil Comportamental, as respostas dadas às perguntas 16 a 17 da parte II do questionário que identificam características do respondente em relação ao seu comportamento perante questões relacionadas à Segurança da Informação.

Tabela 20 - *Model Summary* do Fator 1 (variável dependente) com Perfil Comportamental

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,159	0,025	-0,045	1,030

Fonte: Resultados da pesquisa (2009)

Tabela 21 – ANOVA do Fator 1 (variável dependente) com Perfil Comportamental

	Sum of Squares	df	Mean Square	F	Sig.
Regression	1,894	5	0,379	0,357	0,876
Residual	73,294	69	1,062		
Total	75,188	74			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V16 e V17 demonstram relacionamento com o Fator 1-Usuários, isto é, o Fator 1 não está sendo influenciado pelas variáveis V16 e V17. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil comportamental dos respondentes, inclusive utilizando outras técnicas estatísticas.

A última hipótese a ser testada é a H7 (O perfil organizacional exerce influência significativa perante a adoção de práticas avançadas de Segurança) que relaciona o Fator 1-Usuários com o Perfil Organizacional, conforme resultado apresentado nas tabelas 22 e 23. Para esta pesquisa, considerou-se como Perfil Organizacional, as respostas dadas às perguntas da parte I (V1 a V8) do questionário que identificam características da organização de trabalho do respondente, como unidade da federação, área de atuação, vinculação hierárquica da Segurança da Informação, dentre outras.

Tabela 22 - *Model Summary* do Fator 1 (variável dependente) com Perfil Organizacional

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,635	0,404	0,067	1,04885

Fonte: Resultados da pesquisa (2009)

Tabela 23 – ANOVA do Fator 1 (variável dependente) com Perfil Organizacional

	Sum of Squares	df	Mean Square	F	Sig.
Regression	17,139	13	1,318	1,198	0,340
Residual	25,302	23	1,100		
Total	42,441	36			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V1 a V8 demonstram relacionamento com o Fator 1-Usuários, isto é, o Fator 1 não está sendo influenciado pelas variáveis V1 a V8. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil organizacional dos respondentes, inclusive utilizando outras técnicas estatísticas e eliminando o viés de interpretação ocorrido nas questões V5 (Parque de informática) e V6 (Número estimado de usuários que acessam a rede), conforme relatado na seção 4.1 desta pesquisa (estatística descritiva).

4.3.2 Análise de regressão múltipla para o fator 2-senhas

Em relação à hipótese **H1** (as percepções sobre a facilidade de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), verifica-se o comportamento apresentado nas tabelas 24 e 25 ao relacionar-se a **Facilidade de Uso** das Práticas de Segurança com o Fator 2-Senhas da pesquisa. Para esta pesquisa, considerou-se como facilidade de uso, as respostas dadas às perguntas 18 e 19 da parte III do questionário, ou seja: “V18 - A utilização de práticas de Segurança da Informação requer muito do meu esforço mental”; “V19 - Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação”.

Tabela 24 - *Model Summary* do Fator 2 (variável dependente) com Facilidade de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,316	0,099	-0,0061	1,00

Fonte: Resultados da pesquisa (2009)

Tabela 25 – ANOVA do Fator 2 (variável dependente) com Facilidade de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	7,585	8	0,948	0,942	0,488
Residual	68,414	68	1,006		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

A análise da tabela 24 nos fornece o coeficiente de correlação (R) de 0,316, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,099 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 2-Senhas) é explicado pelas variações na variável independente. Em nosso exemplo, 9,9% da variação no Fator 2 são explicados pelas variações nas variáveis explicativas (V18 e V19).

Os resultados da ANOVA (0,488) indicam que não há evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. Como para este mesmo construto do modelo TAM (Facilidade de Uso) em relação ao fator 1-Usuários houve correlação, estes resultados podem indicar falta de clareza das assertivas da ISO 27001 em relação à utilização de senhas ou, por não ter apresentado a correlação esperada, necessidade de mais pesquisas nesta área.

O comportamento apresentado nas tabelas 26 e 27 é verificado ao relacionar-se a **Utilidade Percebida** das Práticas de Segurança com o Fator 2-Senhas da pesquisa, com vistas a testar a hipótese 2 (As percepções sobre a utilidade de práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança) para este fator. Para esta pesquisa, considerou-se como utilidade percebida, as respostas dadas às perguntas 20 e 21 da parte III do questionário, ou seja: “V20 - Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente”; “V21 - A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho”.

Tabela 26 - *Model Summary* do Fator 2 (variável dependente) com Utilidade Percebida

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,248	0,061	-0,034	1,017

Fonte: Resultados da pesquisa (2009)

Tabela 27 – ANOVA do Fator 2 (variável dependente) com Utilidade Percebida

	Sum of Squares	df	Mean Square	F	Sig.
Regression	4,656	7,000	0,665	0,643	0,719
Residual	71,344	69,000	1,034		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

A análise da tabela 26 nos fornece o coeficiente de correlação (R) de 0,248, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,061 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 2-Senhas) é explicado pelas variações na variável independente. Em nosso exemplo, 6,1% da variação no Fator 2 são explicados pelas variações nas variáveis explicativas (V20 e V21).

Os resultados da ANOVA (sig. 0,719) indicam que não há evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. Como para este mesmo construto do modelo TAM (Utilidade Percebida) em relação ao fator 1-Usuários houve certa correlação (entre os que apresentaram concordância ou os que nem concordavam, nem discordavam), estes resultados podem indicar falta de clareza das assertivas da ISO 27001 em relação à utilização de senhas ou, por não ter apresentado a correlação esperada, necessidade de mais pesquisas nesta área.

Para o fator 2-Senhas em relação à Hipótese H3 (As percepções sobre a atitude perante as práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), verifica-se o comportamento apresentado nos tabelas 28 e 29 ao relacionar-se a **Atitude** perante as Práticas de Segurança. Para esta pesquisa, considerou-se como Atitude, as respostas dadas às perguntas 22 e 23 da parte III do questionário, ou seja: “V22 - Eu gosto de utilizar práticas avançadas de Segurança da Informação”; “V23 - Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante”.

Tabela 28 - *Model Summary* do Fator 2 (variável dependente) com Atitude

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,272	0,074	-0,029	0,935

Fonte: Resultados da pesquisa (2009)

Tabela 29 – ANOVA do Fator 2 (variável dependente) com Atitude

	Sum of Squares	df	Mean Square	F	Sig.
Regression	4,406	7,000	0,629	0,721	0,655
Residual	55,033	63,000	0,874		
Total	59,440	70,000			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V22 e V23 demonstrem relacionamento entre os Fatores analisados. Isto é, o Fator 2-Senhas não está sendo influenciado pelas variáveis independentes (V22 e V23). Isto representa que pessoas com atitude positiva, negativa e neutra perante a adoção de práticas avançadas de Segurança da Informação serão influenciadas da mesma forma por políticas para adoção das referidas práticas. Tais resultados, por não terem apresentado resultados esperados, apontam para necessidade de ampliação de pesquisa em relação ao construto Atitude do Modelo TAM.

Para a hipótese H4 (A intenção de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), a regressão múltipla de fatores apresenta o comportamento exposto nas tabelas 30 e 31 ao relacionar-se o fator 2-Senhas com a **Intenção de Uso** das Práticas de Segurança. Para esta pesquisa, considerou-se como Intenção de Uso, as respostas dadas às perguntas 24 e 25 da parte III do questionário, ou seja: “V24 - Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las”; “V25 - Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria”.

Tabela 30 - *Model Summary* do Fator 2 (variável dependente) com Intenção de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,167	0,028	-0,055	1,027

Fonte: Resultados da pesquisa (2009)

Tabela 31 – ANOVA do Fator 2 (variável dependente) com Intenção de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	2,12	6,00	0,35	0,33	0,92
Residual	73,88	70,00	1,06		
Total	76,00	76,00			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V24 e V25 demonstram relacionamento entre os Fatores analisados. Isto é, o Fator 2-Senhas não está sendo influenciados pelas variáveis independentes (V24 e V25). Isto representa que pessoas com intenção positiva, negativa e neutra perante a adoção de práticas avançadas de Segurança da Informação serão influenciadas da mesma forma por políticas para adoção das referidas práticas. Tais resultados, por não terem apresentado resultados esperados, apontam para necessidade de ampliação de pesquisa em relação ao construto Intenção do Modelo TAM.

Em relação à Hipótese H5 (O perfil demográfico dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança), ao aplicar a regressão múltipla entre o perfil demográfico e o Fator 2-Senhas, verificam-se os resultados apresentados nas tabelas 32 e 33. Para esta pesquisa, considerou-se como Perfil Demográfico, as respostas dadas às perguntas 9 a 15 da parte II do questionário que identificam características do respondente, como sexo, idade, nível de escolaridade, nível de conhecimento em informática, entre outras.

Tabela 32 - *Model Summary* do Fator 2 (variável dependente) com Perfil Demográfico

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,428	0,183	0,058	0,9766

Fonte: Resultados da pesquisa (2009)

Tabela 33 – ANOVA do Fator 2 (variável dependente) com Perfil Demográfico

	Sum of Squares	df	Mean Square	F	Sig.
Regression	13,932	10	1,393	1,461	0,175
Residual	61,995	65	0,954		
Total	75,927	75			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis demográficas (V9 a V15) demonstram relacionamento entre o Fator 2-Senhas, isto é, o Fator 2 não está sendo influenciado pelas variáveis demográficas (V9 a V15). Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil demográfico dos respondentes, inclusive utilizando outras técnicas estatísticas.

Para testar a hipótese H6 (O perfil comportamental dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança) foi realizada análise de regressão do perfil comportamental dos gestores com o Fator 2-Senhas, conforme resultado exposto nas tabelas 34 e 35. Para esta pesquisa, considerou-se como Perfil Comportamental, as respostas dadas às perguntas 16 a 17 da parte II do questionário que identificam características do respondente em relação ao seu comportamento perante questões relacionadas à Segurança da Informação.

Tabela 34 - Model Summary do Fator 2 (variável dependente) com Perfil Comportamental

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,273	0,074	0,007	0,9890

Fonte: Resultados da pesquisa (2009)

Tabela 35 – ANOVA do Fator 2 (variável dependente) com Perfil Comportamental

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	5,420	5	1,084	1,108	0,364
Residual	67,503	69	0,978		
Total	72,924	74			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V16 e V17 demonstram relacionamento com o Fator 2, isto é, o Fator 2 não está sendo influenciado pelas variáveis V16 e V17. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil comportamental dos respondentes, inclusive utilizando outras técnicas estatísticas.

A última hipótese a ser testada em relação ao Fator 2-Senhas é a H7 (O perfil organizacional exerce influência significativa perante a adoção de práticas avançadas de Segurança) que relaciona tal fator com o Perfil Organizacional, conforme resultado

apresentado nas tabelas 36 e 37. Para esta pesquisa, considerou-se como Perfil Organizacional, as respostas dadas às perguntas da parte I (V1 a V8) do questionário que identificam características da organização de trabalho do respondente, como unidade da federação, área de atuação, vinculação hierárquica da Segurança da Informação, dentre outras.

Tabela 36 - Model Summary do Fator 2 (variável dependente) com Perfil Organizacional

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,704	0,496	0,210	0,95300

Fonte: Resultados da pesquisa (2009)

Tabela 37 – ANOVA do Fator 2 (variável dependente) com Perfil Organizacional

	Sum of Squares	df	Mean Square	F	Sig.
Regression	20,517	13	1,578	1,738	0,119)
Residual	20,889	23	0,908		
Total	41,406	36			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V1 a V8 demonstram relacionamento com o Fator 2-Senhas, isto é, o Fator 2 não está sendo influenciado pelas variáveis V1 a V8. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil organizacional dos respondentes, inclusive utilizando outras técnicas estatísticas e eliminando o viés de interpretação ocorrido nas questões V5 (Parque de informática) e V6 (Número estimado de usuários que acessam a rede), conforme relatado na seção 4.1 desta pesquisa (estatística descritiva).

4.3.3 Análise de regressão múltipla para o fator 3-biometria

Em relação à hipótese **H1** (as percepções sobre a facilidade de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança) foram geradas as tabelas 38 e 39 ao se realizar a análise de regressão múltipla. Assim, verifica-se o comportamento apresentado nas referidas Tabelas ao relacionar-se a **Facilidade de Utilização** das Práticas de Segurança com o Fator 3 da

pesquisa. Para esta pesquisa, considerou-se como facilidade de uso, as respostas dadas às perguntas 18 e 19 da parte III do questionário, ou seja: “V18 - A utilização de práticas de Segurança da Informação requer muito do meu esforço mental”; “V19 - Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação”.

Tabela 38 - *Model Summary* do Fator 3 (variável dependente) com Facilidade de Uso

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,384	0,147	0,047	0,976

Fonte: Resultados da pesquisa (2009)

Tabela 39 – ANOVA do Fator 3 (variável dependente) com Facilidade de Uso

	Sum of Squares	**DF**	**Mean Square**	**F**	**Sig.**
Regression	11,196	8,000	1,399	1,468	0,185
Residual	64,804	68,000	0,953		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

A análise da tabela 38 nos fornece o coeficiente de correlação (R) de 0,384, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,147 é denominado coeficiente de determinação ou poder explicativo da regressão. Indica quanto da variação dependente (Fator 3-Biometria) é explicado pelas variações na variável independente. Em nosso exemplo, 14,7% da variação no Fator 3 são explicados pelas variações nas variáveis explicativas (V18 e V19).

Os resultados da ANOVA (sig. 0,185) indicam que não há evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. Como não houve resultados esperados em relação a este construto de modelo TAM (Facilidade de Uso), há indícios de necessidade de ampliação dos estudos nesta área.

O comportamento apresentado nos tabelas 40 e 41 é verificado ao relacionar-se a **Utilidade Percebida** das Práticas de Segurança com o Fator 3-Biometria da pesquisa, com vistas a testar a hipótese 3 (As percepções sobre a utilidade de práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança). Para esta pesquisa, considerou-se como utilidade percebida, as respostas dadas às perguntas 20 e 21 da parte III do questionário, ou seja: “V20 - Adotar práticas de Segurança da

Informação torna meu trabalho mais eficiente"; "V21 - A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho".

Tabela 40 - *Model Summary* do Fator 3 (variável dependente) com Utilidade Percebida

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,320	0,102	0,011	0,994

Fonte: Resultados da pesquisa (2009)

Tabela 41 – ANOVA do Fator 3 (variável dependente) com Utilidade Percebida

	Sum of Squares	df	Mean Square	F	Sig.
Regression	7,784	7,000	1,112	1,125	0,358
Residual	68,216	69,000	0,989		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

A análise da tabela 40 nos fornece o coeficiente de correlação (R) de 0,320, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,102 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 3-Biometria) é explicado pelas variações na variável independente. Em nosso exemplo, 10,2% da variação no Fator 3 são explicados pelas variações nas variáveis explicativas (V20 e V21).

Os resultados da ANOVA (sig. 0,359) indicam que não há evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. Como não houve resultados esperados em relação a este construto de modelo TAM (Utilidade Percebida), há indícios de necessidade de ampliação dos estudos nesta área.

Ao realizar a análise de regressão para o fator 3-Biometria em relação à **Atitude** perante as Práticas de Segurança, com vistas a testar a Hipótese H3 (As percepções sobre a atitude perante as práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), verifica-se o comportamento apresentado nas tabelas 42 e 43. Para esta pesquisa, considerou-se como Atitude, as respostas dadas às perguntas 22 e 23 da parte III do questionário, ou seja: "V22 - Eu gosto de utilizar práticas avançadas de Segurança da Informação"; "V23 - Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante".

Tabela 42 - *Model Summary* do Fator 3 (variável dependente) com Atitude

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,389	0,152	0,057	0,990

Fonte: Resultados da pesquisa (2009)

Tabela 43 – ANOVA do Fator 3 (variável dependente) com Atitude

	Sum of Squares	df	Mean Square	F	Sig.
Regression	11,029	7,000	1,576	1,607	0,150
Residual	61,770	63,000	0,980		
Total	72,799	70,000			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V22 e V23 demonstrem relacionamento com o Fator 3-Biometria, isto é, o Fator 3-Biometria não está sendo influenciado pelas variáveis independentes (V22 e V23). Como não houve resultados esperados em relação a este construto de modelo TAM (Atitude), há indícios de necessidade de ampliação dos estudos nesta área.

Para a hipótese H4 (A intenção de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), a regressão múltipla apresenta o comportamento exposto nas tabelas 44, 45 e 46 ao relacionar-se o Fator 3-Biometria com a **Intenção de Uso** das Práticas de Segurança. Para esta pesquisa, considerou-se como Intenção de Uso, as respostas dadas às perguntas 24 e 25 da parte III do questionário, ou seja: “V24 - Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las”; “V25 - Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria”.

Tabela 44 - *Model Summary* do Fator 3 (variável dependente) com Intenção de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,412	0,169	0,098	0,950

Fonte: Resultados da pesquisa (2009)

Tabela 45 – ANOVA do Fator 3 (variável dependente) com Intenção de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	12,872	6,000	2,145	2,379	0,038
Residual	63,128	70,000	0,902		
Total	76,000	76,000			

Fonte: Resultados da pesquisa (2009)

Tabela 46 – Coefficients do Fator 3 (variável dependente) com Intenção de Uso

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0,631	0,449		1,406	0,164
V 24.2 X1	-2,741	1,415	-0,312	-1,937	0,057
V 24.3 X2	-0,954	0,822	-0,293	-1,161	0,250
V 24.4 X3	-0,867	0,446	-0,432	-1,945	0,056
V 25.2 X1	0,062	0,961	0,010	0,064	0,949
V 25.3 X2	0,790	0,698	0,243	1,132	0,262
V 25.5 X4	-0,261	0,442	-0,123	-0,592	0,556

Fonte: Resultados da pesquisa (2009)

A análise da tabela 44 nos fornece o coeficiente de correlação (R) de 0,412, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,169 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 3-Biometria) é explicado pelas variações na variável independente. Em nosso exemplo, 16,9% da variação no Fator 3 são explicados pelas variações nas variáveis explicativas (V24 e V25).

Os resultados da ANOVA (sig. 0,038) indicam que há fortes evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. A tabela 46 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para V24 (Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las) verifica-se que as variáveis dicotômicas X_1 (discordo) e X_3 (concordo) influenciam no Fator 3-Biometria.

Já a variável V25 (Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria) não mostrou correlação com o Fator 3 (sig. .> 0,10). Isso pode demonstrar necessidade de maior clareza na pergunta do modelo TAM ou

ampliação de pesquisa para este construto (Intenção de Uso). Com isso, o modelo de regressão estimado extraído é:

$$\hat{Y} = -2{,}741X_1 - 0{,}867X_3$$

Do modelo de regressão estimado temos a indicação de que as categorias X_1 e X_3 influenciam de forma negativa no Fator 3-Biometria. Nota-se que a variável X_1 (discorda) e a X_3 (concorda) reduz o Fator 3. Já as demais categorias não apresentaram relação significativa com o Fator 3 (sig. Ou P > 0,10). O resultado apresentado é completamente inesperado, uma vez que pessoas que concordam e discordam da pergunta do Modelo TAM relacionada à Intenção de Uso tem menos propensão a adotar práticas avançadas de Segurança da Informação, enquanto que as pessoas que responderam de forma mais contundente (concordo totalmente ou discordo totalmente) ou até mesmo aquelas com maior neutralidade na questão (nem concordo, nem discordo) não apresentam tal relação. Este resultado aponta para ampliação de estudos em relação a este construto.

Em relação à Hipótese H5 (O perfil demográfico dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança), ao aplicar a regressão múltipla entre o perfil demográfico e o Fator 3-Biometria, verificam-se os resultados apresentados nas tabelas 47 e 48. Para esta pesquisa, considerou-se como Perfil Demográfico, as respostas dadas às perguntas 9 a 15 da parte II do questionário que identificam características do respondente, como sexo, idade, nível de escolaridade, nível de conhecimento em informática, entre outras.

Tabela 47 - *Model Summary* do Fator 3 (variável dependente) com Perfil Demográfico

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,355	0,126	-0,009	0,9996

Fonte: Resultados da pesquisa (2009)

Tabela 48 – ANOVA do Fator 3 (variável dependente) com Perfil Demográfico

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	9,355	10	0,935	0,936	0,507
Residual	64,951	65	0,999		
Total	74,306	75			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis demográficas (V9 a V15) demonstram relacionamento com o Fator 3-Biometria, isto é, o Fator 3 não está sendo influenciado pelas variáveis demográficas (V9 a V15). Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil demográfico dos respondentes, inclusive utilizando outras técnicas estatísticas.

Para testar a hipótese H6 (O perfil comportamental dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança) foi realizada análise de regressão do perfil comportamental dos gestores com o Fator 3-Biometria, conforme resultado exposto nas tabelas 49 e 50. Para esta pesquisa, considerou-se como Perfil Comportamental, as respostas dadas às perguntas 16 a 17 da parte II do questionário que identificam características do respondente em relação ao seu comportamento perante questões relacionadas à Segurança da Informação.

Tabela 49 - *Model Summary* do Fator 3 (variável dependente) com Perfil Comportamental

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,328	0,107	0,043	0,9812

Fonte: Resultados da pesquisa (2009)

Tabela 50 – ANOVA do Fator 3 (variável dependente) com Perfil Comportamental

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	7,996	5	1,599	1,661	0,156
Residual	66,430	69	0,963		
Total	74,426	74			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V16 e V17 demonstram relacionamento com o Fator 3-Biometria, isto é, o Fator 3 não está sendo influenciado pelas variáveis V16 e V17. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil comportamental dos respondentes, inclusive utilizando outras técnicas estatísticas.

A última hipótese a ser testada em relação ao Fator 3-Biometria é a H7 (O perfil organizacional exerce influência significativa perante a adoção de práticas avançadas de Segurança) que relaciona tal fator com o Perfil Organizacional, conforme resultado apresentado nas tabelas 51 e 52. Para esta pesquisa, considerou-se como Perfil

Organizacional, as respostas dadas às perguntas da parte I (V1 a V8) do questionário que identificam características da organização de trabalho do respondente, como unidade da federação, área de atuação, vinculação hierárquica da Segurança da Informação, dentre outras.

Tabela 51 - *Model Summary* do Fator 3 (variável dependente) com Perfil Organizacional

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,505	0,255	-0,167	1,0267

Fonte: Resultados da pesquisa (2009)

Tabela 52 – ANOVA do Fator 3 (variável dependente) com Perfil Organizacional

	Sum of Squares	df	Mean Square	F	Sig.
Regression	8,281	13	0,637	0,604	0,826
Residual	24,247	23	1,054		
Total	32,528	36			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V1 a V8 demonstram relacionamento com o Fator 3-Biometria, isto é, o Fator 3 não está sendo influenciado pelas variáveis V1 a V8. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil organizacional dos respondentes, inclusive utilizando outras técnicas estatísticas e eliminando o viés de interpretação ocorrido nas questões V5 (Parque de informática) e V6 (Número estimado de usuários que acessam a rede), conforme relatado na seção 4.1 desta pesquisa (estatística descritiva).

4.3.4 Análise de regressão múltipla para o fator 4-férias

Para o fator 4, verifica-se a hipótese **H1** (as percepções sobre a facilidade de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança) através da análise do comportamento ao relacionar-se a **Facilidade de Utilização** das Práticas de Segurança nas tabelas 53 e 54. Para esta pesquisa, considerou-se como facilidade de uso, as respostas dadas às perguntas 18 e 19

da parte III do questionário, ou seja: “V18 - A utilização de práticas de Segurança da Informação requer muito do meu esforço mental”; “V19 - Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação”.

Tabela 53 - *Model Summary* do Fator 4 (variável dependente) com Facilidade de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,243	0,059	-0,052	1,026

Fonte: Resultados da pesquisa (2009)

Tabela 54 – ANOVA do Fator 4 (variável dependente) com Facilidade de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	4,473	8	0,559	0,532	0,829
Residual	71,527	68	1,052		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

A análise da tabela 53 nos fornece o coeficiente de correlação (R) de 0,243, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,059 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 4-Férias) é explicado pelas variações na variável independente. Em nosso exemplo, 5,9% da variação no Fator 4 são explicados pelas variações nas variáveis explicativas (V18 e V19).

Os resultados da ANOVA (sig. 0,829) indicam que não há evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. Este resultado pode indicar maior clareza na pergunta que formulou o fator 4-Férias ou ampliação de pesquisa em relação ao construto do Modelo TAM (Facilidade de Uso).

Para testar a hipótese 2 (As percepções sobre a utilidade de práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), relaciona-se a **Utilidade Percebida** das Práticas de Segurança com o Fator 4-Férias da pesquisa, verifica-se o comportamento apresentado nas tabelas 55, 56 e 57. Para esta pesquisa, considerou-se como utilidade percebida, as respostas dadas às perguntas 20 e 21 da parte III do questionário, ou seja: “V20 - Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente”; “V21 - A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho”.

Tabela 55 - *Model Summary* do Fator 4 (variável dependente) com Utilidade Percebida

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,517	0,267	0,193	0,899

Fonte: Resultados da pesquisa (2009)

Tabela 56 – ANOVA do Fator 4 (variável dependente) com Utilidade Percebida

	Sum of Squares	df	Mean Square	F	Sig.
Regression	20,294	7,000	2,899	3,591	0,002
Residual	55,706	69,000	0,807		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

Tabela 57 – *Coefficients* do Fator 4 (variável dependente) com Utilidade Percebida

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-1,430	0,982		-1,456	0,150
V20.2 (X1)	-0,715	0,437	-0,207	-1,635	0,107
V20.3 (X2)	-0,360	0,396	-0,156	-0,910	0,366
V20.4 (X3)	-0,056	0,310	-0,028	-0,180	0,858
V20.5 (X4)	1,040	0,981	0,319	1,060	0,293
V21.2 (X5)	1,404	0,954	0,560	1,472	0,146
V21.3 (X6)	1,955	0,950	0,982	2,059	0,043
V21.4 (X7)	1,436	0,982	0,600	1,462	0,148
V21.5 (X8)	-1,430	0,982		-1,456	0,150

Fonte: Resultados da pesquisa (2009)

A análise da tabela 55 nos fornece o coeficiente de correlação (R) de 0,517, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,267 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 4-Férias) é explicado pelas variações na variável independente. Em nosso exemplo, 26,7% da variação no Fator 4 são explicados pelas variações nas variáveis explicativas (V20 e V21).

Os resultados da ANOVA (sig. 0,002) indicam que há fortes evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. A tabela 57 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para o relacionamento descrito no modelo apenas uma categoria dicotômica da variável V20 (Adotar práticas de

Segurança da Informação torna meu trabalho mais eficiente) não houve significância relevante. Isto pode indicar dificuldades de interpretação no conceito de eficiência. Para o relacionamento descrito no modelo apenas uma categoria dicotômica da variável V21 (A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho) foi significativa para compor o modelo. Com isso, o modelo de regressão estimado extraído é:

$$\hat{Y} = 1,955X_6$$

O modelo de regressão estimado indica que a categoria nem discordo e nem concordo da V21 influencia de forma positiva no Fator 4-Férias. Já as demais categorias não apresentaram relação significativa com o Fator 4 (sig. Ou P > 0,10). Este resultado demonstra que as pessoas que possuem neutralidade na opinião sobre a utilidade percebida, estão mais dispostas a adotar práticas avançadas de Segurança da Informação. Isto pode indicar que tais pessoas percebem as práticas de Segurança da Informação como algo do cotidiano e não como algo extremamente útil ou o contrário.

Ao realizar a análise de regressão para o Fator 4-Férias em relação à **Atitude** perante as Práticas de Segurança, conforme Hipótese H3 (As percepções sobre a atitude perante as práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), verifica-se o comportamento apresentado nas tabelas 58, 59 e 60. Para esta pesquisa, considerou-se como Atitude, as respostas dadas às perguntas 22 e 23 da parte III do questionário, ou seja: “V22 - Eu gosto de utilizar práticas avançadas de Segurança da Informação”; “V23 - Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante”.

Tabela 58 - *Model Summary* do Fator 4 (variável dependente) com Atitude

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,533	0,284	0,204	0,912

Fonte: Resultados da pesquisa (2009)

Tabela 59 – ANOVA do Fator 4 (variável dependente) com Atitude

	Sum of Squares	df	Mean Square	F	Sig.
Regression	20,786	7,000	2,969	3,568	0,003
Residual	52,424	63,000	0,832		
Total	73,210	70,000			

Fonte: Resultados da pesquisa (2009)

Tabela 60 – *Coefficients* do Fator 4 (variável dependente) com Atitude

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-0,718	0,579		-1,240	0,220
V22.2 (X1)	-1,427	0,791	-0,489	-1,803	0,076
V22.3 (X2)	-0,442	0,733	-0,213	-0,603	0,549
V22.4 (X3)	-0,478	0,721	-0,227	-0,663	0,509
V22.5 (X4)	-0,078	0,864	-0,018	-0,090	0,928
V23.2 (X5)	0,874	0,780	0,333	1,121	0,267
V23.3 (X6)	1,308	0,721	0,636	1,815	0,074
V23.4 (X7)	1,594	0,736	0,750	2,166	0,034
V23.5 (X8)	-0,718	0,579		-1,240	0,220

Fonte: Resultados da pesquisa (2009)

A análise da tabela 58 nos fornece o coeficiente de correlação (R) de 0,533, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,284 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 4-Férias) é explicado pelas variações na variável independente. Em nosso exemplo, 28,4% da variação no Fator 4 são explicados pelas variações nas variáveis explicativas (V22 e V23).

Os resultados da ANOVA (sig. 0,003) indicam que há fortes evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. A tabela 60 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para o relacionamento descrito no modelo da variável V22 (Eu gosto de utilizar práticas avançadas de Segurança da Informação) apenas uma categoria dicotômica X_1 (discordo) foi significativa para compor o modelo. Para a variável V23 (Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante) tem-se a variável X_6 e X_7. Com isso, o modelo de regressão estimado extraído é:

$$\hat{Y} = -1,427X_1 + 1,308X_6 + 1,594X_7$$

O modelo de regressão estimado indica que a categoria X_1 (discordo) influencia de forma negativa no Fator 4-Férias. Assim, quanto mais a pessoa gosta de utilizar práticas avançadas de Segurança da Informação, mais propensa ela será a adotá-las. Com relação à variável V23 tem-se que as categorias X_6 (discordo) e X_7 (nem concordo, nem discordo) influenciam no Fator 4-Férias de forma negativa. Já as demais categorias não apresentaram relação significativa com o Fator 4 (sig. Ou P > 0,10). Tal resultado demonstra que quanto menor a discordância ou a neutralidade sobre a percepção de que o trabalho fica mais interessante com a utilização de práticas avançadas de Segurança da Informação, maior será o índice de adoção da referida norma.

Para a hipótese H4 (A intenção de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), a regressão múltipla de fatores apresenta o comportamento exposto nas tabelas 61 e 62 ao relacionar-se o Fator 4-Férias com a **Intenção de Uso** das Práticas de Segurança. Para esta pesquisa, considerou-se como Intenção de Uso, as respostas dadas às perguntas 24 e 25 da parte III do questionário, ou seja: "V24 - Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las"; "V25 - Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria".

Tabela 61 - *Model Summary* do Fator 4 (variável dependente) com Intenção de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,208	0,043	-0,039	1,019

Fonte: Resultados da pesquisa (2009)

Tabela 62 – ANOVA do Fator 4 (variável dependente) com Intenção de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	3,293	6,000	0,549	0,528	0,785
Residual	72,707	70,000	1,039		
Total	76,000	76,000			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V24 e V25 demonstram relacionamento entre o Fator 4-Férias, isto é, o Fator 4 não está sendo influenciado pelas variáveis independentes (V24 e V25). Este resultado não esperado aponta para necessidade de ampliação de pesquisa em relação a este construto e verificação da clareza da assertiva da ISO 27001 utilizada nesta pesquisa para gerar o fator 4-Férias.

Em relação à Hipótese H5 (O perfil demográfico dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança), ao aplicar a regressão múltipla entre o perfil demográfico e o Fator 4-Férias, verificam-se os resultados apresentados nas tabelas 63 e 64. Para esta pesquisa, considerou-se como Perfil Demográfico, as respostas dadas às perguntas 9 a 15 da parte II do questionário que identificam características do respondente, como sexo, idade, nível de escolaridade, nível de conhecimento em informática, entre outras.

Tabela 63 - *Model Summary* do Fator 4 (variável dependente) com Perfil Demográfico

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,364	0,133	-0,001	1,0058

Fonte: Resultados da pesquisa (2009)

Tabela 64 – ANOVA do Fator 4 (variável dependente) com Perfil Demográfico

	Sum of Squares	df	Mean Square	F	Sig.
Regression	10,068	10	1,007	0,995	0,457
Residual	65,764	65	1,012		
Total	75,831	75			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis demográficas (V9 a V15) demonstram relacionamento com o Fator 4-Férias, isto é, o Fator 4-Férias não está sendo influenciado pelas variáveis demográficas (V9 a V15). Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil demográfico dos respondentes, inclusive utilizando outras técnicas estatísticas.

Para testar a hipótese H6 (O perfil comportamental dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança) foi realizada

análise de regressão do perfil comportamental dos gestores com o Fator 4-Férias, conforme resultado exposto nas tabelas 65 e 66. Para esta pesquisa, considerou-se como Perfil Comportamental, as respostas dadas às perguntas 16 a 17 da parte II do questionário que identificam características do respondente em relação ao seu comportamento perante questões relacionadas à Segurança da Informação.

Tabela 65 - *Model Summary* do Fator 4 (variável dependente) com Perfil Comportamental

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,250	0,063	-0,005	0,99681

Fonte: Resultados da pesquisa (2009)

Tabela 66 – ANOVA do Fator 4 (variável dependente) com Perfil Comportamental

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	4,581	5	0,916	0,922	0,472
Residual	68,562	69	0,994		
Total	73,142	74			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V16 e V17 demonstram relacionamento com o Fator 4-Férias, isto é, o Fator 4 não está sendo influenciado pelas variáveis V16 e V17. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil comportamental dos respondentes, inclusive utilizando outras técnicas estatísticas.

A última hipótese a ser testada em relação ao Fator 4-Férias é a H7 (O perfil organizacional exerce influência significativa perante a adoção de práticas avançadas de Segurança) que relaciona tal fator com o Perfil Organizacional, conforme resultado apresentado nas tabelas 67, 68 e 69. Para esta pesquisa, considerou-se como Perfil Organizacional, as respostas dadas às perguntas da parte I (V1 a V8) do questionário que identificam características da organização de trabalho do respondente, como unidade da federação, área de atuação, vinculação hierárquica da Segurança da Informação, dentre outras.

Tabela 67 - *Model Summary* do Fator 4 (variável dependente) com Perfil Organizacional

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,732	0,535	0,273	0,87655

Fonte: Resultados da pesquisa (2009)

Tabela 68 – ANOVA do Fator 4 (variável dependente) com Perfil Organizacional

	Sum of Squares	df	Mean Square	F	Sig.
Regression	20,356	13	1,566	2,038	0,066
Residual	17,672	23	0,768		
Total	38,028	36			

Fonte: Resultados da pesquisa (2009)

Tabela 69 – *Coefficients* do Fator 4 (variável dependente) com Perfil Organizacional

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-1,0540	0,9720		-1,0850	0,2890
V 3.2 (X1)	0,7680	0,7510	0,3780	1,0230	0,3170
V 3.3 (X2)	0,7420	0,7550	0,3140	0,9830	0,3360
V 3.4 (X3)	-0,2910	1,0430	-0,0650	-0,2790	0,7830
V 3.5 (X4)	0,3890	0,8270	0,1420	0,4710	0,6420
V 3.6 (X5)	1,1310	1,1880	0,1810	0,9520	0,3510
V5 (X6)	-0,0001	0,0000	-0,1310	-0,6350	0,5320
V6 (X7)	0,0000	0,0000	0,5110	2,8230	0,0100
V 7.2 (X8)	0,1050	0,5190	0,0490	0,2030	0,8410
V 7.3 (X9)	-0,4250	0,5080	-0,2030	-0,8380	0,4110
V 7.4 (X10)	-1,2370	0,6390	-0,3790	-1,9370	0,0650
V 8.2 (X11)	0,5260	0,3910	0,2580	1,3450	0,1920
V 8.3 (X12)	0,6600	0,6500	0,2020	1,0150	0,3210
V 8.4 (X13)	1,0260	0,7140	0,2290	1,4370	0,1640

Fonte: Resultados da pesquisa (2009)

A análise da tabela 67 nos fornece o coeficiente de correlação (R) de 0,732, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,535 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 4-Férias) é explicado pelas variações na variável independente. Em nosso exemplo, 53,6% da variação no Fator 4 são explicados pelas variações nas variáveis explicativas (V1 e V8).

A tabela de regressão que fornece ANOVA apresenta teste do efeito do conjunto de variáveis independentes sobre a variável dependente. Este teste consiste em se verificar a probabilidade de que os parâmetros da regressão em conjunto são iguais a zero,

existindo assim uma relação estatística significativa. Pelo sig deste caso (0,06), constata-se que o modelo apresenta um R^2 significativamente diferente de zero (sig razoavelmente baixo), ou pelo menos um dos coeficientes do modelo é diferente de zero. Em outras palavras, os resultados da ANOVA (0,06) indicam que há relacionamento linear entre a variável dependente e o conjunto de variáveis independentes.

A tabela 69 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para o relacionamento descrito no modelo apenas as variáveis V6 e V7, com a categoria dicotômica X_4, foi significativa para compor o modelo, mas a variável V6 prejudica o modelo, pois mostra que existe correlação, mas o coeficiente é zero, isto deve-se ao fato de valores muito diferenciados já explicados na seção 4.1 deste estudo (Estatística Descritiva), relativas ao parque computacional e usuários da rede. Diante de tal limitação, optou-se por descartar este modelo e não considerar a significância apontada na relação. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil organizacional dos respondentes, inclusive utilizando outras técnicas estatísticas e eliminando o viés de interpretação ocorrido nas questões V5 (Parque de informática) e V6 (Número estimado de usuários que acessam a rede), conforme já relatado.

4.3.5 Análise de regressão múltipla para o fator 5-desligamento

Para a hipótese **H1** (as percepções sobre a facilidade de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), verificam-se os resultados de análise de regressão múltipla do fator 5 em relação à **Facilidade de Uso** das Práticas de Segurança apresentados nas tabelas 70, 71 e 72. Para esta pesquisa, considerou-se como facilidade de uso, as respostas dadas às perguntas 18 e 19 da parte III do questionário, ou seja: “V18 - A utilização de práticas de Segurança da Informação requer muito do meu esforço mental”; “V19 - Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação”.

Tabela 70 - *Model Summary* do Fator 5 (variável dependente) com Facilidade de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,438	0,192	0,097	0,950

Fonte: Resultados da pesquisa (2009)

Tabela 71 – ANOVA do Fator 5 (variável dependente) com Facilidade de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	14,584	8,000	1,823	2,018	0,057
Residual	61,416	68,000	0,903		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

Tabela 72 – *Coefficients* do Fator 5 (variável dependente) com Facilidade de Uso

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-0,714	0,351		-2,033	0,046
V18.2 (X1)	-0,003	0,308	-0,001	-0,010	0,992
V18.3 (X2)	0,140	0,317	0,065	0,442	0,660
V18.4 (X3)	0,241	0,387	0,081	0,622	0,536
V18.5 (X4)	0,133	0,735	0,021	0,181	0,857
V19.2 (X5)	0,447	0,397	0,190	1,124	0,265
V19.3 (X6)	0,662	0,390	0,305	1,698	0,094
V19.4 (X7)	0,639	0,396	0,277	1,613	0,111
V19.5 (X8)	1,717	0,473	0,527	3,629	0,001

Fonte: Resultados da pesquisa (2009)

A análise da tabela 70 nos fornece o coeficiente de correlação (R) de 0,438, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,192 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 5-Desligamento) é explicado pelas variações na variável independente. Em nosso exemplo, apenas 19,2% da variação no Fator 5 são explicados pelas variações nas variáveis explicativas (V18 e V19).

Os resultados da ANOVA (sig. 0,057) indicam que há fracas evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes.

A tabela 72 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para o relacionamento descrito no modelo apenas a variável V19 (Eu tenho muita facilidade em

utilizar práticas avançadas de Segurança da Informação), com exceção das duas categorias dicotômicas X_5 e X_7, foi significativa para compor o modelo. Este resultado pode indicar dificuldade da interpretação da pergunta V18 relacionada ao modelo TAM, pois a mesma não apresentou correlação significante. Com isso, o modelo de regressão estimado extraído é:

$$\hat{Y} = -0,714 + 0,662X_6 + 1,717X_8$$

O modelo de regressão estimado indica que a V19 influencia de forma positiva no Fator 5-Desligamento, isto é, a variável V19 e o Fator 5 estão correlacionados positivamente. Quanto maior a facilidade de uso percebida, haverá maior concordância em adotar práticas avançadas de Segurança da Informação. Nota-se que X_6 (nem concorda e nem discorda), em média, aumenta o Fator 5 em 0,66, e a X_8 (concorda totalmente) aumenta o Fator 5 em 1,71. Já as demais categorias não apresentaram relação significativa com o Fator 5 (sig. Ou P > 0,10).

Para verificar a hipótese 2 (As percepções sobre a utilidade de práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança) em relação ao fator 5-Desligamento, é feita a análise de seu relacionamento com a **Utilidade Percebida** das Práticas de Segurança. Os resultados são apresentados nos tabelas 73 e 74. Para esta pesquisa, considerou-se como utilidade percebida, as respostas dadas às perguntas 20 e 21 da parte III do questionário, ou seja: "V20 - Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente"; "V21 - A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho".

Tabela 73 - *Model Summary* do Fator 5 (variável dependente) com Utilidade Percebida

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	0,323	0,105	0,014	0,993

Fonte: Resultados da pesquisa (2009)

Tabela 74 – ANOVA do Fator 5 (variável dependente) com Utilidade Percebida

	Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
Regression	7,947	7,000	1,135	1,151	0,342
Residual	68,053	69,000	0,986		
Total	76	76			

Fonte: Resultados da pesquisa (2009)

A análise da tabela 73 nos fornece o coeficiente de correlação (R) de 0,323, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,105 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 5-Desligamento) é explicado pelas variações na variável independente. Em nosso exemplo, 10,5% da variação no Fator 5 são explicados pelas variações nas variáveis explicativas (V20 e V21). Os resultados da ANOVA (sig. 0,342) indicam que não há evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes. Tal resultado difere da correlação esperada, indicando necessidade de ampliação de estudos deste construto do Modelo TAM (Utilidade Percebida) e verificação da clareza na redação da assertiva da norma ISO 27001 que compõe este fator.

Em relação à Hipótese H3 (As percepções sobre a atitude perante as práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), foi realizada a regressão para o fator 5-Desligamento. Assim, verifica-se o comportamento apresentado nas tabelas 75, 76 e 77 ao relacionar-se a **Atitude** perante as Práticas de Segurança com tal fator. Para esta pesquisa, considerou-se como Atitude, as respostas dadas às perguntas 22 e 23 da parte III do questionário, ou seja: "V22 - Eu gosto de utilizar práticas avançadas de Segurança da Informação"; "V23 - Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante".

Tabela 75 - *Model Summary* do Fator 5 (variável dependente) com Atitude

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	**0,472**	**0,223**	**0,136**	**0,935**

Fonte: Resultados da pesquisa (2009)

Tabela 76 – ANOVA do Fator 5 (variável dependente) com Atitude

	Sum of Squares	df	Mean Square	F	Sig.
Regression	15,770	7,000	2,253	2,578	0,021
Residual	55,049	63,000	0,874		
Total	70,819	70,000			

Fonte: Resultados da pesquisa (2009)

Tabela 77 – *Coefficients* do Fator 5 (variável dependente) com Atitude

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-1,588	0,593		-2,678	0,009
V22.2 (X1)	2,159	0,811	0,752	2,663	0,010
V22.3 (X2)	2,330	0,751	1,140	3,102	0,003
V22.4 (X3)	2,347	0,738	1,132	3,178	0,002
V22.5 (X4)	2,705	0,885	0,624	3,055	0,003
V23.2 (X5)	-1,038	0,799	-0,402	-1,299	0,199
V23.3 (X6)	-0,754	0,738	-0,373	-1,022	0,311
V23.4 (X7)	-0,474	0,754	-0,227	-0,629	0,532
V23.5 (X8)	-1,588	0,593		-2,678	0,009

Fonte: Resultados da pesquisa (2009)

A análise da tabela 75 nos fornece o coeficiente de correlação (R) de 0,475, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,223 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 5-Desligamento) é explicado pelas variações na variável independente. Em nosso exemplo, 22,3% da variação no Fator 5 são explicados pelas variações nas variáveis explicativas (V22 e V23). Os resultados da ANOVA (sig. 0,021) indicam que há fortes evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes.

A tabela 77 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para o relacionamento descrito no modelo da variável V22 (Eu gosto de utilizar práticas avançadas de Segurança da Informação) com o Fator 5-Desligamento, verifica-se que essa variável influencia de forma positiva tal fator, ou seja, quanto mais o respondente gosta de utilizar práticas avançadas de Segurança da Informação, mais propenso ele é a adotar as referidas práticas.

Para a variável V23 (Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante), apenas a variável dicotômica X_8 (concordo totalmente) foi significativa. Com isso, o modelo de regressão estimado extraído é:

$$\hat{Y} = -1,588\mathrm{X}_1 + 2,159X_2 + 2,330X_2 + 2,344X_3 + 2,705X_4 - 1,588X_8$$

O modelo de regressão estimado indica que as categorias X_1, X_2, X_3 e X_4 influenciam de forma positiva no Fator 5. Com relação à variável V23 tem-se que X_8 influencia de forma negativa no Fator 5. Já as demais categorias não apresentaram relação significativa com o Fator 5 (sig. Ou P > 0,10). Isto indica que apenas uma atitude positiva (concordo totalmente) sobre a percepção de que a adoção de práticas deixa o trabalho mais interessante, gera tal correlação. Assim, tais pessoas apresentam maior aceitação de práticas avançadas de segurança em relação a desligamento de usuários da organização (fator 5).

Em relação à hipótese H4 (A intenção de utilização das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança), percebe-se o comportamento exposto nas tabelas 78, 79 e 80 ao relacionar o Fator 5-Desligamento com a **Intenção de Uso** das Práticas de Segurança. Para esta pesquisa, considerou-se como Intenção de Uso, as respostas dadas às perguntas 24 e 25 da parte III do questionário, ou seja: "V24 - Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las"; "V25 - Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria".

Tabela 78 - *Model Summary* do Fator 5 (variável dependente) com Intenção de Uso

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,480	0,231	0,165	0,914

Fonte: Resultados da pesquisa (2009)

Tabela 79 – ANOVA do Fator 5 (variável dependente) com Intenção de Uso

	Sum of Squares	df	Mean Square	F	Sig.
Regression	17,522	6,000	2,920	3,496	0,004
Residual	58,478	70,000	0,835		
Total	76,000	76,000			

Fonte: Resultados da pesquisa (2009)

Tabela 80 – *Coefficients* do Fator 5 (variável dependente) com Intenção de Uso

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0,500	0,432		1,158	0,251
V 24.2 X1	-0,146	1,362	-0,017	-0,107	0,915
V 24.3 X2	-1,166	0,791	-0,358	-1,473	0,145

V 24.4 X3	-0,726	0,429	-0,362	-1,693	0,095
V 25.2 X1	1,334	0,925	0,214	1,441	0,154
V 25.3 X2	-0,087	0,672	-0,027	-0,129	0,898
V 25.5 X4	0,037	0,425	0,017	0,087	0,931

Fonte: Resultados da pesquisa (2009)

A análise da tabela 78 nos fornece o coeficiente de correlação (R) de 0,480, que representa o grau de associação entre as variáveis dependente e independente. O valor de R Square = 0,231 é denominado coeficiente de determinação ou poder explicativo da regressão. Ele indica quanto da variação dependente (Fator 5-Desligamento) é explicado pelas variações na variável independente. Em nosso exemplo, 23,1% da variação no Fator 5 são explicados pelas variações nas variáveis explicativas (V24 e V25). Os resultados da ANOVA (sig. 0,004) indicam que há fortes evidências de que o modelo ajustado demonstra relacionamento entre a variável dependente e as independentes.

A tabela 80 (*Coefficients*) nos dá a confirmação da significância de cada um dos coeficientes isoladamente e nos permite escrever o modelo de regressão estimado. Para a variável V24 (Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-la), verifica-se que apenas a variável dicotômica X_3 (concordo) apresenta uma fraca influencia no Fator 5 (sig. = 0,095). Nota-se que a variável X_3 reduz o Fator 5-Desligamento em 0,726. Já na variável V25 (Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria) nenhuma variável dicotômica influencia o Fator 5. Com isso, o modelo de regressão estimado extraído é:

$$\hat{Y} = -0,726X_3$$

O fato da concordância com a pergunta do modelo TAM representar redução no fator, ou seja, na concordância em adotar as práticas avançadas de Segurança da Informação, representam necessidade de ampliação de pesquisa com este construto, uma vez que tal resultado difere do esperado.

Em relação à Hipótese H5 (O perfil demográfico dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança), ao aplicar a regressão múltipla entre o perfil demográfico e o Fator 5-Desligamento, verificam-se os resultados apresentados nas tabelas 81 e 82. Para esta pesquisa, considerou-se como Perfil Demográfico, as respostas dadas às perguntas 9 a 15 da parte II do questionário que

identificam características do respondente, como sexo, idade, nível de escolaridade, nível de conhecimento em informática, entre outras.

Tabela 81 - *Model Summary* do Fator 5 (variável dependente) com Perfil Demográfico

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,413	0,170	0,043	0,963

Fonte: Resultados da pesquisa (2009)

Tabela 82 – ANOVA do Fator 5 (variável dependente) com Perfil Demográfico

	Sum of Squares	df	Mean Square	F	Sig.
Regression	12,365	10	1,237	1,333	0,232
Residual	60,294	65	0,928		
Total	72,659	75			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis demográficas (V9 a V15) demonstram relacionamento com o Fator 5-Desligamento, isto é, o Fator 5 não está sendo influenciado pelas variáveis demográficas (V9 a V15). Assim, como demonstrado nas seções anteriores, para nenhum dos fatores da pesquisa houve demonstração de relacionamento significante entre a variável dependente e o perfil demográfico dos respondentes. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil demográfico dos respondentes, inclusive utilizando outras técnicas estatísticas.

Para testar a hipótese H6 (O perfil comportamental dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança) foi realizada análise de regressão do perfil comportamental dos gestores com o Fator 5-Desligamento, conforme resultado exposto nas tabelas 83 e 84. Para esta pesquisa, considerou-se como Perfil Comportamental, as respostas dadas às perguntas 16 a 17 da parte II do questionário que identificam características do respondente em relação ao seu comportamento perante questões relacionadas à Segurança da Informação.

Tabela 83 - *Model Summary* do Fator 5 (variável dependente) com Perfil Comportamental

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,097	0,009	-0,062	1,0053

Fonte: Resultados da pesquisa (2009)

Tabela 84 – ANOVA do Fator 5 (variável dependente) com Perfil Comportamental

	Sum of Squares	df	Mean Square	F	Sig.
Regression	,666	5	0,133	0,132	0,985
Residual	69,738	69	1,011		
Total	70,404	74			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V16 e V17 demonstram relacionamento com o Fator 5-Desligamento, isto é, o Fator 5 não está sendo influenciado pelas variáveis V16 e V17. Assim, da mesma forma que a hipótese 5, a hipótese 6 não pode ser comprovada pela pesquisa porque para nenhum dos fatores houve correlação significativa com as variáveis independentes, conforme demonstrado nas seções anteriores. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil comportamental dos respondentes, inclusive utilizando outras técnicas estatísticas.

A última hipótese a ser testada em relação ao Fator 5-Desligamento é a H7 (O perfil organizacional exerce influência significativa perante a adoção de práticas avançadas de Segurança) que relaciona tal fator com o Perfil Organizacional, conforme resultado apresentado nas tabelas 85 e 86. Para esta pesquisa, considerou-se como Perfil Organizacional, as respostas dadas às perguntas da parte I (V1 a V8) do questionário que identificam características da organização de trabalho do respondente, como unidade da federação, área de atuação, vinculação hierárquica da Segurança da Informação, dentre outras.

Tabela 85 - *Model Summary* do Fator 5 (variável dependente) com Perfil Organizacional

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,421	0,177	-0,288	0,97525

Fonte: Resultados da pesquisa (2009)

Tabela 86 – ANOVA do Fator 5 (variável dependente) com Perfil Organizacional

	Sum of Squares	df	Mean Square	F	Sig.
Regression	4,705	13	0,362	0,381	0,963
Residual	21,876	23	0,951		
Total	26,581	36			

Fonte: Resultados da pesquisa (2009)

As análises dos resultados da ANOVA indicam que não há evidências de que as variáveis V1 a V8 demonstram relacionamento com o Fator 5-Desligamento, isto é, o Fator 5 não está sendo influenciado pelas variáveis V1 a V8. Na seção seguinte é apresentado um resumo dos resultados da regressão linear em relação à validação das hipóteses de pesquisa, bem como seu relacionamento com a teoria estudada para desenvolvimento desta pesquisa. Tais resultados apontam para necessidade de ampliação de pesquisa em relação ao perfil organizacional dos respondentes, inclusive utilizando outras técnicas estatísticas e eliminando o viés de interpretação ocorrido nas questões V5 (Parque de informática) e V6 (Número estimado de usuários que acessam a rede), conforme relatado na seção 4.1 desta pesquisa (estatística descritiva).

4.4 VALIDAÇÃO DAS HIPÓTESES PROPOSTAS

O quadro 11 abaixo demonstra a validação das hipóteses em relação a cada um dos fatores apresentados na seção anterior.

Hipóteses	Fator	Situação
H1) As percepções sobre a **facilidade de utilização** das práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança	1-Usuários	Confirmada
	2-Senhas	Não confirmada
	3-Biometria	Não confirmada
	4-Férias	Não confirmada
	5-Desligamento	Confirmada
H2) As percepções sobre a **utilidade** de práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança	1-Usuários	Confirmada
	2-Senhas	Não confirmada
	3-Biometria	Não confirmada
	4-Férias	Confirmada
	5-Desligamento	Não confirmada

H3) As percepções sobre a **atitude** perante as práticas de Segurança exercem uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança	1-Usuários	Não confirmada
	2-Senhas	Não confirmada
	3-Biometria	Não confirmada
	4-Férias	Confirmada
	5-Desligamento	Confirmada
H4) A **intenção** de utilização das práticas de Segurança exerce uma influência positiva significativa sobre a adoção de práticas avançadas de Segurança	1-Usuários	Não confirmada
	2-Senhas	Não confirmada
	3-Biometria	Confirmada
	4-Férias	Não confirmada
	5-Desligamento	Confirmada
H5) O **perfil demográfico** dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança	1-Usuários	Não confirmada
	2-Senhas	Não confirmada
	3-Biometria	Não confirmada
	4-Férias	Não confirmada
	5-Desligamento	Não confirmada
H6) O **perfil comportamental** dos gestores exerce influência significativa perante a adoção de práticas avançadas de Segurança	1-Usuários	Não confirmada
	2-Senhas	Não confirmada
	3-Biometria	Não confirmada
	4-Férias	Não confirmada
	5-Desligamento	Não confirmada
H7) O **perfil organizacional** exerce influência significativa perante a adoção de práticas avançadas de Segurança	1-Usuários	Não confirmada
	2-Senhas	Não confirmada
	3-Biometria	Não confirmada
	4-Férias	Não confirmada
	5-Desligamento	Não confirmada

Quadro 11 – Validação das hipóteses
Fonte: Próprio autor (2009)

Verifica-se que em cada uma das hipóteses relacionadas ao Modelo TAM (H1 a H4) houve confirmação em dois fatores, conforme a seguir:

- H1 (construto TAM: Facilidade de uso): Fator 1-Usuários e Fator 5-Desligamento;
- H2 (construto TAM: Utilidade Percebida): Fator 1-Usuários e Fator 4-Férias;
- H3 (construto TAM: Atitude): Fator 4-Férias e Fator 5-Desligamento;
- H4 (construto TAM: Intenção em Utilizar): Fator 2-Biometria e Fator 5-Desligamento.

Pode-se, portanto, considerar que tais hipóteses H1, H2, H3 e H4 foram confirmadas, destacando a seguinte confirmação em relação aos fatores:

- Fator 1-Usuários: confirmou duas hipóteses (H1 e H2);
- Fator 2-Senhas: não confirmou nenhuma hipótese;
- Fator 3-Biometria: confirmou uma hipótese (H4);
- Fator 4-Férias: confirmou duas hipóteses (H2 e H3);
- Fator 5-Desligamento: confirmou três hipóteses (H1, H3 e H4).

Tais resultados apontam para forte significância do fator 5 no modelo proposto e fraca relevância do fator 2 no referido modelo. Este fato pode ser revisto em pesquisas futuras para analisar a clareza das respectivas assertivas, além da correlação.

Após a apresentação dos resultados, torna-se importante a verificação de tais resultados à luz da teoria estudada para formatar o modelo de pesquisa utilizado. Assim, podemos reconhecer se os relacionamentos significativos encontrados neste estudo corroboram ou vão de encontro a estudos anteriores.

No caso da **hipótese 1** que aponta para a influência da percepção de **facilidade de uso** na adoção de práticas avançadas de segurança, ou seja, testa o relacionamento entre V18 (A utilização de práticas de Segurança da Informação requer muito do meu esforço mental) e V19 (Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação) com os fatores que representam a concordância em utilização da norma, encontrou-se correlação do construto do modelo TAM em relação ao Fator 1-Usuários e 5-Desligamento, positivamente. Daí pode-se concluir que quanto maior a facilidade em utilizar práticas avançadas de Segurança, maior será a concordância com a adoção de normas de segurança. Tal resultado é corroborado por pesquisas anteriores que também concluíram que a percepção de facilidade de uso interfere positivamente na adoção de tecnologias (VENKATESH; DAVIS, 1996; VENKATESH, 2000; VENKATESH; DAVIS, 2000; DAVIS; VENKATESH, 2004). Apesar de Venkatesh *et al.* (2003) defender que a facilidade de uso é o construto que perdeu a força de sua significância ao longo dos anos, nesta pesquisa ele ainda foi comprovado como relacionamento significante com a variável dependente através dos fatores 1 e 5.

No caso da **hipótese 2** que aponta para a influência da percepção de **utilidade percebida** na adoção de práticas avançadas de segurança, ou seja, testa o relacionamento entre V20 (Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente) e V21 (A utilização de práticas de Segurança da Informação é extremamente importante para a

realização do meu trabalho) com os fatores que representam a concordância em utilização da norma, encontrou-se correlação entre o comportamento das variáveis independentes (V20 e V21) em relação aos Fatores 1-Usuários e 4-Férias, positivamente. Daí pode-se concluir que quanto maior a utilidade percebida nas práticas, maior será a concordância com a adoção de normas de segurança. Tal resultado é corroborado por pesquisas anteriores que também concluíram que a utilidade percebida interfere positivamente na adoção de tecnologias (DAVIS; VENKATESH, 2004).

No caso da **hipótese 3** que aponta para a influência da **atitude** na adoção de práticas avançadas de segurança, ou seja, testa o relacionamento entre V22 (Eu gosto de utilizar práticas avançadas de Segurança da Informação) e V23 (Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante) com os fatores que representam a concordância em utilização da norma, encontrou-se correlação entre o comportamento das variáveis independentes em relação aos Fatores 4-Férias e 5-Desligamento, positivamente. Daí pode-se concluir que quanto mais positiva for a atitude perante as práticas avançadas, maior será a concordância com a adoção de normas de segurança. Venkatesh *et al.* (2004) além de reforçar a significância de outros construtos do modelo TAM, destaca a importância da atitude, especialmente para o sexo masculino. Já Oliveira Junior (2007) aponta este construto como de relevância fraca no modelo, no entanto, como explanado, ele obteve resultados de correlação significante nesta pesquisa. No entanto, vale destacar que ambos os fatores que confirmaram esta hipótese, 4-Férias e 5-Desligamento, são formados por apenas uma assertiva da norma cada um, V2 e V12, respectivamente, portanto, recomenda-se aprofundamento de estudo nesta área.

No caso da **hipótese 4** que aponta para a influência da **intenção de uso** de adoção de práticas avançadas de segurança, ou seja, testa o relacionamento entre V24 (Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las) e V25 (Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria) com os fatores que representam a concordância em utilização da norma, encontrou-se correlação entre o comportamento das variáveis independentes em relação aos Fatores 2-Biometria e 5-Desligamento. O modelo TAM postula que a intenção de utilizar uma tecnologia é determinada pela utilidade percebida. Portanto, este resultado de confirmação da hipótese confirma o modelo teórico adotado para esta pesquisa com base em estudos anteriores (DAVIS; VENKATESH, 2004). No entanto, vale destacar que ambos os fatores que confirmaram esta hipótese, 3-Biometria e 5-Desligamento, são formados por apenas uma

assertiva da norma cada um, V13 e V12, respectivamente, portanto, recomenda-se aprofundamento de estudo nesta área.

No caso da **hipótese 5** que aponta para a influência do **perfil demográfico** dos gestores públicos de adoção de práticas avançadas de segurança, ou seja, testa o relacionamento entre V9 a V15 (perguntas 9 a 15 do questionário que caracterizam os respondentes quanto a idade, sexo, formação etc.) com os fatores que representam a concordância em utilização da norma, não foi verificado relacionamento significante entre as variáveis independentes e os fatores da pesquisa que têm correspondência com as assertivas da norma ISO 27001. Tanto Venkatesh e Morris (2000a), quanto e Venkatesh, Morris, Sykes e Ackerman (2004) encontraram resultados diferentes deste quando comprovaram que o sexo é uma variável que influencia a aceitação de tecnologias. Já Venkatesh e Morris (2000b) detectaram que a idade é um fator relevante na aceitação de tecnologias. Venkatesh, Morris e Ackerman (2000) além da variável sexo também encontraram significância nas variáveis renda, posição na organização, educação e experiência em relação a adoção de tecnologias, ou seja, tais autores defendem que estas variáveis exercem influência em tal adoção. Por não ter encontrado os resultados esperados, recomenda-se estudos complementares, inclusive utilizando outras técnicas estatísticas como análise de cluster, por exemplo.

No caso da **hipótese 6** que aponta para a influência do **perfil comportamental** dos gestores públicos de adoção de práticas avançadas de segurança, ou seja, testa o relacionamento entre V16 e V17 (perguntas 16 e 17 do questionário que caracterizam os respondentes quanto aos seus comportamentos em situações de adoção de Segurança da Informação) com os fatores que representam a concordância em utilização da norma, não foi verificado relacionamento significante entre as variáveis independentes e os fatores da pesquisa, que correspondência as assertivas da norma ISO 27001. Não foram encontrados estudos anteriores que testaram o relacionamento de variáveis de comportamento em relação à Segurança da Informação como os desta pesquisa, para que se faça a comparação. Assim, como não houve nenhuma relação significante entre tais variáveis e os fatores gerados por esta pesquisa, pode-se concluir este estudo como demonstração de que tal relacionamento não é significante e, em estudos futuros, pode-se tentar comprovar ou rejeitar esta afirmação.

No caso da **hipótese 7** que aponta para a influência do **perfil organizacional** de adoção de práticas avançadas de segurança, ou seja, testa o relacionamento entre V1 a V8 (perguntas 1 a 8 do questionário que caracterizam a organização do respondente quanto a localização, hierarquia do setor de SI etc.) com os fatores que representam a concordância em utilização da norma, não foi verificado relacionamento significante entre as variáveis

independentes e os fatores da pesquisa que correspondência as assertivas da norma ISO 27001. Dias, Zwicker e Vicentin (2003) apontam como deficiência do Modelo TAM, a falta de investigação da área organizacional. Este estudo tentou suprimir esta lacuna, uma vez que não foram encontrados estudos anteriores que testassem o relacionamento de variáveis como porte da organização, região geográfica, existência de estrutura formal de setor de SI e outras. Assim, não foi possível fazer comparação. Como já demonstrado neste capítulo, a análise da hipótese 7 ficou comprometida por falhas nas interpretações nas perguntas quantitativas do perfil organizacional. Além disso, há pouca variabilidade em duas variáveis categóricas e outra apresenta um nível de desconhecimento alto. Tal situação inviabiliza, portanto, interpretação e não permite fazer qualquer predição a respeito da interferência das variáveis que compõem o perfil organizacional com a adoção de práticas avançadas de segurança.

Os resultados da pesquisa apresentados podem ser utilizados de forma prática para direcionar investimentos para adoção de políticas de segurança da informação através do foco na obtenção de características do modelo TAM para os membros de uma organização pública, especialmente quando formada por gestores das áreas foco desta pesquisa (planejamento e gestão). Assim, antes de realizar implantações de práticas avançadas de Segurança da Informação, pode ser verificado qual o nível de cada um dos construtos do modelo para o corpo funcional da organização e antes do início da implantação adotar medidas para elevar os níveis de tais construtos (facilidade de uso, utilidade percebida, atitude e intenção em utilizar).

Diante dos resultados, recomenda-se que para ampliar a facilidade de uso, sejam realizados treinamentos básicos e palestras sobre o tema. Para aumentar a percepção de utilidade da Segurança da Informação, sejam divulgados informativos sobre os riscos da insegurança. Para melhorar o nível de atitude e intenção em utilizar práticas de SI, sejam feitas palestras de sensibilização, inclusive utilizando pessoas do quadro funcional da própria organização.

Estas ações devem fazer parte da rotina das organizações públicas com vistas a direcionar investimentos e evitar desperdícios, implantando políticas onerosas, que por falta de preparação do ambiente, através de atividades simples, não atinjam seus objetivos.

5. CONSIDERAÇÕES FINAIS

Esta pesquisa iniciou com um relato sobre a evolução da importância da informação nas organizações e, consequentemente, a manutenção de tais informações seguras. A Gestão de Segurança da Informação tornou-se um tema relevante nos ambientes organizacionais sejam eles públicos ou privados (SÊMOLA; 2003).

No decorrer da pesquisa houve algumas limitações, sendo uma delas o baixo índice de devolução dos questionários de gestores de organizações especialistas em TI (Diretores das filiadas à ABEP), o que resultou no descarte das referidas ocorrências. A análise de tais dados permitiria verificar se a aceitação dos gestores de organizações especialistas em TI pode, de alguma forma, interferir na adoção de práticas avançadas de Segurança da Informação e na percepção dos demais gestores (coordenadores do PNAGE), relacionando-se os dois grupos. Esta estratégia mostrou-se mal sucedida e poderia ter sido substituída pela investigação com os responsáveis de TI das organizações onde o PNAGE está inserido. Acredita-se que, adotando tal público no lugar dos Diretores das organizações filiadas à ABEP, o quantitativo de questionários respondidos seria mais alto e o relacionamento entre os dois públicos poderia ter sido testado. Para trabalhos futuros, sugere-se adotar gestores internos como público especialista em TI.

Outra limitação que pode ser apontada foi a falta de clareza em duas questões referentes ao perfil organizacional (número de equipamentos do parque de informática e número de usuários que acessam a rede), não detectadas no pré-teste. Isto resultou em interpretação equivocada. Para tais questões houve três tipos de resposta. Alguns responderam em relação ao setor de trabalho, outros de todo o Governo do Estado e apenas uma parte como se esperava, ou seja, da organização de trabalho (órgão, empresa etc.). Além da falha de interpretação, tais perguntas tiveram um índice considerável de omissões, o que inviabilizou os testes que deveriam ser feitos. Como forma de correção para trabalhos futuros, sugere-se deixar a questão mais clara ou obter tais números através de dados secundários.

A pesquisa confirma as quatro hipóteses relacionadas ao Modelo TAM que são: facilidade de uso, utilidade percebida, atitude e intenção de uso, sendo que as duas últimas carecem estudos futuros, por terem sido comprovadas pelo relacionamento com fatores formados por apenas uma assertiva da norma, cada um. Apesar disso, considera-se que as variáveis do Modelo TAM exercem significativa influência na adoção de práticas

avançadas de Segurança da Informação. Já as três hipóteses relacionadas ao perfil demográfico e comportamental dos gestores públicos e o perfil organizacional não tiveram comprovação de significância e seus testes foram prejudicados pelas limitações já mencionadas. Diante de tais resultados, o modelo da pesquisa pode ser revisado, conforme Diagrama 10, no qual as hipóteses confirmadas permanecem (H1, H2, H3 e H4), enquanto as hipóteses não confirmadas são sinalizadas com marcação correspondente (H5, H6, H7).

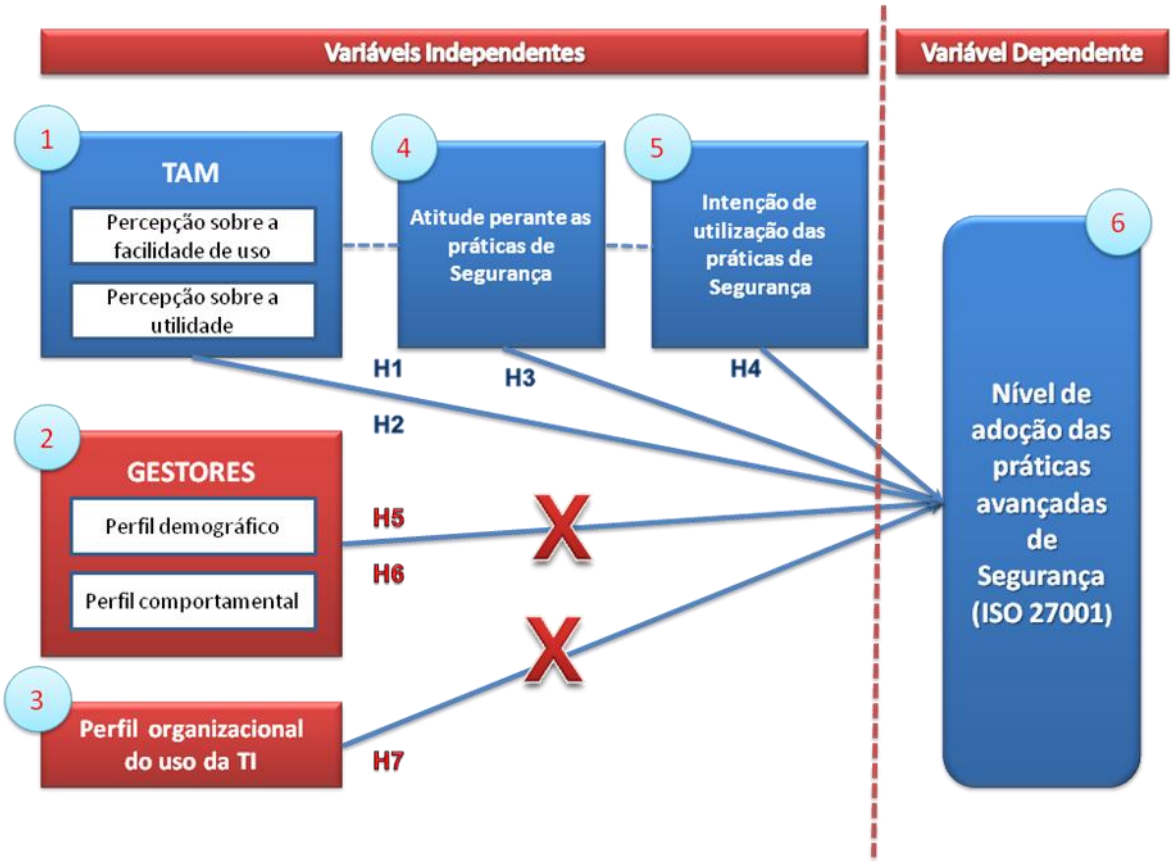


Diagrama 10 – Modelo teórico da pesquisa revisto
Fonte: Próprio autor (2009)

Esta pesquisa utilizou um público específico de gestores públicos que são os das áreas administrativas e de planejamento e, portanto, seus resultados só devem ser considerados para tal público. Assim, abre-se um leque de oportunidades de trabalhos futuros, como por exemplo, realizar estudos com gestores públicos de outras áreas, como: tributação, saúde, educação e segurança públicas. Além de tais estudos isoladamente, pode-se realizar relacionamentos entre públicos distintos e com gestores especialistas em TI. As hipóteses que não foram confirmadas também podem ser utilizadas em estudos futuros.

Trabalhos desta natureza exercem um papel extremamente relevante tanto do ponto de vista teórico, quanto prático e social. A relevância teórica se apresenta pelo modelo adotado e a metodologia que pode ser replicada, além de ser um aprofundamento numa área onde há escassez de trabalhos (aceitação de práticas avançadas de Segurança da Informação).

A contribuição prática deste tipo de trabalho é dada por ele poder ser utilizado como norteador de políticas e investimentos públicos. Já a contribuição social, se dá pelo direito à informação que todo cidadão brasileiro possui. Este é um dos principais direitos do cidadão, tanto que está previsto no art. 5º da Constituição Federal, que trata das garantias e direitos constitucionais da pessoa. O inciso XXXIII de tal artigo, relata: "todos têm o direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral...". Este direito ainda decorre do princípio da publicidade ou transparência, descrito no art. 37 da mesma Constituição, ou seja, ele é um direito originário de um princípio orientador da função pública.

É através da informação que se garante a plena cidadania e assegurar que ela esteja íntegra, confiável e disponível é dever de qualquer gestor público. Ao se conhecer quais são os fatores que influenciam os gestores públicos na aceitação de práticas de Segurança da Informação, podem ser adotadas medidas mais focadas e que tragam resultados mais concretos, obtendo-se ganho social.

REFERÊNCIAS

ASSMANN, R. **A gestão da segurança do trabalho sob a ótica da teoria da complexidade**. 2006. 115 f. Dissertação (Mestrado em Administração) – Universidade Federal de Santa Catarina, Florianópolis. 2006.

AKUTSU, L.; PINHO, J. A. G. de. Sociedade da informação, accountability e democracia delegativa. **Revista de Administração Pública**, Rio de Janeiro, v. 36, n. 5, p. 723-745, 2002.

ALMEIDA, F.J.R.; SOBRAL, F.J.B.A. Os condicionantes psicológicos e estruturais da informatização organizacional: um estudo sobre empresas portuguesas utilizando o modelo de equações estruturais. REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 29., 2005, Brasília. *Anais...* Brasília: ANPAD, 2005.

ASCIUTTI, C. A. **Alinhando ABNT-NBR-ISO/IEC 17799 e 27001 para a administração pública**. São Paulo: Agência USP de Inovação, 2006.

BALANCED SCOREDCARD INSTITUTE. Disponível em <http://www.balancedscorecard.org/#>. Acesso em: 27 abr. 2009.

BALDISSERA, T. A.; NUNES, R. C. Impacto na implementação da norma ISO/IEC 17799 para a gestão da segurança da informação em colégios**:** um estudo de caso**.** XXVII ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO, 27., 2007, Foz do Iguaçu. *Anais…* Foz do Iguaçu: Associação Brasileira de Engenharia da Produção, 2007.

BARNERS-LEE, T. **The world wide webs**: past, present and future. Disponível em: <http://www.w3.org/People/Berners-Lee/1996/ppf.html >. World Wide Web Consortium. Acesso em: 02 jun. 2009.

BARNUM, G. Availability, access, authenticity, and persistence: creating the environment for permanent public access to electronic government information. Washington: **Government Information Quarterly**, n. 19, p. 37-43, 2002.

BAUER, C.A. **Política de segurança da informação para redes corporativas**. 2006. 71 f. Trabalho de Conclusão de Curso (Graduação em Ciências da Computação) – Instituto de Ciências Exatas e Tecnológicas, Centro Universitário FEEVALE, Novo Hamburgo. 2006.

BROWN, S. A.; VENKATESH, V; BALA, H. Household technology use: integrating household life cycle and the model of adoption of technology in holseholds. Minneapolis: **MIS Quartely**, v. 29, n. 3, p. 399-426, 2005.

BUENO, U.; ZWICKER, R.; OLIVEIRA, M.A. Um estudo comparativo do modelo de aceitação aplicado em sistemas de informação e comércio eletrônico. CONGRESSO INTERNACIONAL DE GESTÃO DE TECNOLOGIA E SISTEMAS DE INFORMAÇÃO, 1., 2004, São Paulo. *Anais...* São Paulo: USP, 2004.

CAMPOS, A. N. **Sistema de segurança da informação**. Florianópolis: Visual Books, 2006.

CARVALHO, R.B.; FERREIRA, M.A.T. Avaliação da qualidade de intranets e portais corporativos: proposta de modelo e pesquisa exploratória em médias e grandes organizações. XXIX REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 29., 2005, Brasília. *Anais...* Brasília: ANPAD, 2005.

CARVALHO, R.C. **A aplicação de um modelo de gestão de segurança da informação e a sua influência na percepção de competitividade no setor de telecomunicações e informática**. 2003. 210 f. Dissertação (Mestrado em Engenharia da Produção), Universidade Federal Fluminense, Rio de Janeiro. 2003.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CAVALCANTE, S.M. **Segurança da informação no correio eletrônico com base na ISO/IEC 17799**: um estudo de caso em uma instituição superior com foco no treinamento. 2003. 133 f. Dissertação (Mestrado em Engenharia da Produção), Universidade Federal do Rio Grande do Norte, Natal. 2003.

CAVUSOGLU, H., B. MISHRA, S. RAGHUNATHAN. A Model for Evaluating IT Security Investments. **Communications of the ACM**, v. 47, n.7, p. 87-92, 2004.

CERT. **Cert research annual report**. Pittsburgh: Software Engineering Institute – Carnegie Mellon. Disponível em: <http://www.cert.org/research/2008research-report.pdf>. Acesso em: 29 maio 2009.

COMMON CRITERIA RECOGNITION AGREEMENT. **Common Criteria**. Disponivel em: <http://www.commoncriteriaportal.org/thecc.html>. Acesso em: 09 jun. 2009.

CORRAR, L. J.; PAULO, E.; DIAS FILHO, J. M.. **Análise multivariada para os cursos de administração, ciências contábeis e economia**, São Paulo: Atlas, 2007.

COSTA FILHO, B. A.; PIRES, P. J. Revisitando os caixas-automáticos: o modelo TAM (technology acceptancy model) aplicado aos ATM´S. XXVIII REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 28., 2004, Curitiba. *Anais...* Curitiba: ANPAD, 2004.

_____. Avaliação de fatores relacionados na formação de índice de prontidão à tecnologia: TRI (technology readiness index) como antecedentes do modelo TAM (tecchnology acceptancy model). XXIX REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 29., 2005, Brasília. *Anais...* Brasília: ANPAD, 2005.

CUNHA, M. A. V. C.; DUCLÓS, L. C.; CORREA, S. M.; SOUZA, G. S. O uso de meios eletrônicos no relacionamento do parlamentar com o cidadão e com o Poder Executivo nos grandes municípios brasileiros. In: EnANPAD, XXIX. Brasília, 2005. **Anais…** Rio de Janeiro, ANPAD, 2005.

CURTI, J.C. **Análise de segurança em aplicações que utilizam plataformas UNIX e MS-Windows no modelo Cliente/Servidor.** 2004. 158 f. Dissertação (Mestrado em Computação) – Instituto de Computação, Universidade Estadual de Campinas. 2004.

D´ANDREA, E. R. P. Segurança da Informação: uma visão estratégica para as organizações. In: ALBERTIN, A. L.; MOURA, R. M. (Orgs.). **Tecnologia da Informação**. São Paulo: Atlas, p.255-277, 2004.

DAVIS, F. D.; VENKATESH, V. Toward preprototype user acceptance testing of new information systems: implications for software project management. **IEEE Transactions on Engineering Management,** v. 51, n. 1, p. 31-46, 2004.

DOD. **Department of defense trusted computer system evaluation criteria**. Disponível em: <http://fas.org/irp/nsa/rainbow/std001.htm>. USA Departament of Defense. Acesso em: 02 set. 2008.

DIAS, M. C.; ZWICKER, R.; VICENTIN, I. C. Análise do modelo de aceitação de tecnologia de Davis. Curitiba: **R. Spei**, v. 4, n. 2, p. 15-23, 2003.

EUROPEAN COMMUNITIES**. Information technology security evaluation criteria (itsec):** provisional harmonised criteria. Disponível em: <http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf >. Office for Official Publications of the European Communities, Bruxelas: ECSC-EEC-EAEC, ISBN 92-826-3004-8, 1991. Acesso em: 18 set. 2008.

FERREIRA, F. N. F. **Segurança da informação**. Rio de Janeiro: Ciência Moderna Ltda., 2003.

FONSECA, M.V.M. **Alinhamento estratégico da tecnlologia**. 2003. 140 f. Dissertação (Mestrado em Administração de Empresas) - Departamento de Administração, Pontifícia Universidade Católica, Rio de Janeiro. 2003.

FONTES, E. **A difícil opção pela proteção da informação.** 2005. Disponível em: <http://www.firewalls.com.br/>. Acesso em: 01 out. 2006.

FRÓIO, L.R. **Um modelo faseado de gestão de segurança da informação**. 2008. 145 f. Dissertação (Mestrado em Engenharia Elétrica) – Faculdade de Tecnologia, Universidade de Brasília, Brasília. 2008.

GABBAY, M. S. **Fatores influenciadores da implementação de ações de gestão de segurança da informação**: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte. 2003. 169 f. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal do Rio Grande do Norte, Natal, 2003.

GOODE, W. J.; HATT, P. K. **Métodos em Pesquisa Social**. 6. ed. São Paulo: Editora Nacional, 1977.

GORE, Al. Creación de uma ciudad eletrônica mundial. Barcelona: **Papers de Formació Municipal**, n. 52, 1998.

HAIR *et al.* **Análise Multivariada de Dados**. 5. ed. Porto Alegre: Bookman, 2005.

IEC. **History**. International Engineering Consortium. Disponível em: <http:\\www.iec.org/about/history.html> Acesso em: 01 maio 2008.

ISACA. Disponível em <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>. Acesso em: 02 ago. 2009.

ISO. **ISO 27000.** International Organization for Standartization. Disponível em: <http://www.27000.org/ismsprocess.htm>. Acesso em: 10 jun 2009.

ITIL. Disponível em <http://www.itil-officialsite.com/home/home.asp>. Acesso em: 09 jun. 2009.

JOIA, L.A. Developing government-to-government enterprises in Brazil: a heuristic model drawn from multiple case studies. International. Rio de Janeiro: **Journal of Information Management**, v. 24, p. 147-166, 2004.

LAUREANO, M. A. P. **Gestão de segurança da informação.** Disponível em: <http://www.laureano.eti.br/ensino/puc/gst/gestao_da_seguranca_da_informacao-v20.pdf#search=%22laureano%20A%20pr%C3%B3xima%20figura%20demonstra%2C%20do%20ponto%20de%20vista%20estrat%C3%A9gico%2C%22>. Acesso em: 01 out. 2006.

LESSA, B.M. **Gestão estratégica da segurança da informação**. 2004. 56 f. Monografia (Especialização em Tecnologia da Informação) – Gerência de TI, Universidade FUMEC, Belo Horizonte. 2004.

LIMA, L.F.F.M. **Percepção de segurança em sistemas de informação e sua relação com a qualidade percebida de serviços, perfil de liderança e perfil dos seguidores, entre as diretorias do INMETRO**. 2006. Dissertação (Mestrado em Engenharia da Produção) – Universidade Federal Fluminense, Rio de Janeiro. 2006.

LÖBLER, M.L.; VISENTINI, M.S.; VIEIRA, K.M. A aceitação do comércio eletrônico explicado pelos modelos TAM e TIF combinados. XXX REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

LORENS, E.M. **Aspectos normativos da segurança da informação**: um modelo de cadeia de regulamentação. 2007. 144 f. Dissertação (Mestrado em Ciência da Informação) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2007.

LUCAS JUNIOR, H. C. **Tecnologia da informação:** tomada de decisão estratégica para administradores. Rio de Janeiro: LTC, 2006.

MACADAR, M.A.; REINHARD, N. **Telecentros Comunitários possibilitando a Inclusão Digital:** um estudo de caso comparativo de iniciativas brasileiras. XXVI

REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 26., 2002, Salvador. *Anais...* Salvador: ANPAD, 2002.

MARCONI, M. de A.; LAKATOS, E. M. **Técnicas de pesquisa**. 4. ed. São Paulo: Atlas S.A, 1999.

MARTINS; A.B. **Uma abordagem metodológica baseada em normas e padrões de segurança**: estudo de caso Cetrel S/A. Salvador: Cetrel S.A. - Empresa Proteção Ambiental Polo Petroquímico da Bahia, 2007. Disponível em <http://www.exatec.unisinos.br/~leo/arquivos/seginfo/P03_ssi04.pdf>. CETREL. Acesso em: 05 jul. 2008.

MENDONÇA, M.C.S. **A percepção gerencial sobre o modelo de gestão de segurança da informação de uma empresa pública de TIC:** perspectiva de evolução para um modelo de governança. 2007. 185 f. Dissertação (Mestrado em Gestão do Conhecimento e Tecnologia da Informação), Universidade Católica de Brasília, Brasília. 2007.

MENEZES, J.C. **Gestão de segurança da informação**: análise em três organizações brasileiras. 2005. 103 f. Dissertação (Mestrado Profissional em Administração) – Escola de Administração, Universidade Federal da Bahia, Salvador. 2005.

MPOG-BRASIL. **Apresentação do PNAGE**. Disponível em: <http://www.planejamento.gov.br/secretaria.asp?cat=171&sec=14>. Ministério do Planejamento, Orçamento e Gestão do Brasil. Acesso em: 01 maio de 2008.

MIRANDA, S.V.; STREIT, R.E. **O processo de gestão da informação em organizações públicas.** ENCONTRO DE ADMINISTRAÇÃO DA INFORMAÇÃO, 1., 2007, Florianópolis. *Anais...* Florianópolis: ANPAD, 2007.

MODULO. **10ª pesquisa nacional de segurança da informação**. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Modulo Security. Acesso em: 01 maio 2009.

MONTGOMERY, D. C.; PECK, E. A. **Introduction to linear regression analysis**. 2. ed. New York: John Wiley e Sons, 1992. 527p.

MOON, M. J. The evolution of e-governement among municipalities: rethoric ou reality? Texas: **Public Administration Review**, v. 62, n. 4, p. 424-433, 2002.

MOREIRA, Nilton S. **Segurança Mínima**: uma visão corporativa da segurança de informações. Rio de Janeiro, Axcel Books, 2001.

MORRIS, M. G.; VENKATESH, V. Age differences in technology adoption decicions: implications for a changing work force. College Park: **Personnel Psychology**. v. 53, n. 2, p. 375-403, 2000.

NAKAMURA, E. T.; DE GEUS, P. L. **Segurança de redes em ambientes cooperativos**. Futura, 2003.

NIÑO, F. M. **A oferta de serviços turísticos nos ambientes de comércio online e offline**. 2001. 216 f. Tese (Doutorado em Administração), Universidade de São Paulo, São Paulo, 2009.

O´BRIEN, J. A. **Sistemas de informação e as decisões gerenciais na era da internet**. 9 ed., São Paulo: Saraiva, 2001.

OCDE. El governo del futur: resum del simposi. Barcelona: **Papers de Formació Municipal,** n. 78, 2001.

OLIVEIRA, B.M.K.; RAMOS, A.S.M. **Padrão de uso do *e-learning* a partir do modelo de aceitação de tecnologia**: uma pesquisa com alunos do curso a distância de graduação em administração da UFRN. V CONGRESSO VIRTUAL BRASILEIRO DE ADMINISTRAÇÃO., 5., 2008, Natal. *Anais...* São Paulo: COVINBRA, p. 18, 2008.

OLIVEIRA, J. P. M. Informação, informática e sociedade. São Paulo: **Revista São Paulo em Perspectiva, Fundação Estadual de Análise de Dados**. SEADE, v. 8, n. 4, p. 6, 1994.

OLIVEIRA, L.C.A; CUNHA, M.A.V.C; SANTOS FILHO, H.P. A tecnologia da informação na relação entre o estado e o cidadão: a expectativa dos excluídos digitais num estudo de caso no estado do Paraná. XXVII REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 27., 2003, Atibaia. *Anais...* Atibaia: ANPAD, 2003.

OLIVEIRA, L.C.B.; JOIA, L.A. **Uma proposta de modelo para avaliação de websites do comércio eletrônico**: aplicação ao varejo virtual de CD´s. XXVIII REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 28., 2004, Curitiba. *Anais...* Curitiba: ANPAD, 2004.

OLIVEIRA, S. L. **Tratado de metodologia científica**. São Paulo: Pioneira, 1997.

OLIVEIRA JUNIOR, R.S. **Avaliação de aceitação de sistemas integrados de gestão**. ENCONTRO DE ADMINISTRAÇÃO DA INFORMAÇÃO, 1., 2007, Florianópolis. *Anais...* Florianópolis: ANPAD, 2007.

PIRES, P.J.; YAMAMOTO, C.S; COSTA FILHO, B.A. Avaliação e reespecificação de um modelo unificado de aceitação da tecnologia da informação (UTAUT) a partir de usuários de um sistema de voz sobre protocolo IP. XXX REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

PLANO EDITORIAL. Anuário da Revista TI & Governo 2005. **TI & GOVERNO**. 2005. 58 p.

QUINTELLA, H. M.; PELICCIONE, F. **Análise dos fatores críticos de sucesso no lançamento do multi-protocol label switching (mpls) no mercado de telecomunicações para serviços aéreos brasileiros**. Disponível em: <www.producao.uff.br/conteudo/rpep/.../RelPesq_V6_2006_10.doc>. Universidade Federal Fluminense. Acesso em: 06 maio 2009.

RAMOS, I. Q. **Contribuição da ciência da informação para criação de um plano de segurança da informação**. 2007. 117 f. Dissertação (Mestrado em Ciência da Informação) – Pontifícia Universidade Católica de Campinas (PUC), Campinas. 2007.

RODRIGUES, E.T.; COSTA, I.S.A. Valores individuais: uma lente conceitual para o estudo do uso da tecnologia da informação nas organizações. XXX REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

RUEDIGER, M. A. Governo eletrônico e democracia: uma análise preliminar dos impactos e potencialidades na gestão pública. XXX REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

SANTOS, L.D.; AMARAL, L.A.M. Determinantes do sucesso de adopção e difusão de serviços de informação online. V CONFERÊNCIA DA ASSOCIAÇÃO PORTUGUESA DE SISTEMAS DE INFORMAÇÃO, 5., 2004, Lisboa. *Atas...* Lisboa: APSI, 2004, 13 p.

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

SILVA, A.L.M.R.; DIAS, D.S. Influência do treinamento de usuários na aceitação de sistemas ERP no Brasil. XXX REUNIÃO ANUAL DA ASSOCIAÇÃO NACIONAL DE PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 30., 2006, Salvador. *Anais...* Salvador: ANPAD, 2006.

SILVA, P. M. Modelo de aceitação de tecnologia (TAM) aplicado ao Sistema de Informação da Biblioteca Virtual em Saúde (BVS) nas Escolas de Medicina da Região Metropolitana do Recife. **Informação & Sociedade**. Estudos, v. 19, p. 117-117, 2009.

SILVA, P.M.G. A função auditoria de sistemas de informação: modelo funcional e de competências. 2008. 192 f. Tese (Mestrado em Tecnologias e Sistemas de Informação) – Escola de Engenharia, Universidade do Minho, Braga, 2008.

SILVA, P. M.; DIAS, G. A., SENA JUNIOR, M. R. A importância da cultura na adoção tecnológica: o caso do technology acceptance model (TAM). Florianópolis: **Revista Eletrônica de Biblioteconomia e Ciência da Informação**, v. 13, n. 26, p 1-7, 2008.

SILVA NETTO, A. Gestão de segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. 2007. 106 f. Dissertação (Mestrado em Administração) – Universidade Municipal de São Caetano do Sul, São Caetano do Sul. 2007.

SOUZA, R.M. **Implantação de ferramentas e técnicas de segurança da informação em conformidade com as normas ISO 27001 e 17799**. 2007. 131 f. Dissertação (Mestrado em Gestão de Redes e Telecomunicações) – Centro de Ciências Exatas, Ambientais e de Tecnologias, Pontifícia Universidade Católica de Campinas, Campinas. 2007.

STAIR, R. M.; REYNOLDS, G. W. **Princípios de sistemas de informação.** 4. ed. Rio de Janeiro: LTC, 2002.

TCU-BRASIL. 3 ed. **Boas práticas em segurança da informação**: Tribunal de Contas da União. Brasília: TCU - Secretaria de Fiscalização de Tecnologia da Informação, 2008.

TURBAN, E.; RAINER, R. K.; POTTER, R. E. **Administração da tecnologia da informação:** teoria e prática. Rio de Janeiro: Campus, 2003.

VASCONCELOS, L. **Adoção de inovações**: o uso do *e-learning* por colaboradores de uma empresa de telecomunicações. 2008. 252 f. Tese (Doutorado em Administração) – Faculdade de Economia, Administração e Contabilidade (FEA), Universidade de São Paulo, São Paulo, 2008.

VASCONCELOS, R.; RICCIO, E, L. Desafios da governança em tecnologia da informação. CONGRESSO INTERNACIONAL DE GESTÃO DE TECNOLOGIA E SISTEMAS DE INFORMAÇÃO, 1., 2004, São Paulo. *Anais*... São Paulo: USP, 2004.

VAZ, J.C. **Desafios para a inclusão digital e governança eletrônica.** São Paulo: Instituto Polis, 2002.

VENKATESH, V. **Models**. Disponível em: <http://www.vvenkatesh.com/organizations/models.asp>. Acesso em: 07 jun. 2009.

_____. Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. Maryland: **Information Systems Research**, v. 11, n. 4, 2000, p. 342–365.

_____. A critical assessment of potencial measurement biases in the technology acceptance model: three experiments. Maryland: **J-Human computer studies**, v. 45, 1996, p. 19–45.

VENKATESH, V.; DAVIS, F. D. A model of the antecedents of perceived ease of use: development and test. North St Paul: **Decision Sciences,** v. 23, n. 2, p. 451-481, 1996.

_____. A theoretical extension of the technology acceptance model: four longitudinal field studies. Philadelphia: **Management Science 2000 INFORMS**, v. 46, n. 2, p. 186–204, 2000.

VENKATESH, V.; MORRIS, G. M. Why don't men ever stop to ask for directions? gender, social influence, and their role in technology acceptance and usage behavior. Minneapolis: **MIS Quarterly**, v. 24 n. 1, p. 115-139, 2000.

_____. Age differences in technology adoption decisions: implications for a changin work force. Minneapolis: **MIS Quarterly**, v. 24 n. 1, 2000, p. 375-403.

VENKATESH, V.; MORRIS, G. M.; ACKERMAN, P.L. A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. East Lansing: **Organizational Behavior and Human Decision Processes,** v. 83, n. 1, p. 33–60, 2000.

VENKATESH, V.; MORRIS, G. M.; SYKES, T.A.; ACKERMAN, P.L. Individual reactions in the workplace: the role of gender as a psychological construct. Arlington: **Journal of Applied Social Psychology**, v. 34, n. 3, p. 445-467, 2004.

VENKATESH *et al.* User acceptance of information technology: toward a unified view. Minneapolis: **MIS Quarterly**, v. 27 n. 3, p. 425-478, 2003.

VIEIRA, W. O. O uso do ITIL para governança de TI: resumo. CONGRESSO INTERNACIONAL DE GESTÃO DE TECNOLOGIA E SISTEMAS DE INFORMAÇÃO, 1., 2004, São Paulo. *Anais...* São Paulo: USP, 2004.

APÊNDICES

Apêndice A – Questionário aplicado com Gestores do PNAGE

Nº

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS - DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO

FATORES QUE INFLUENCIAM A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO: Um Estudo com Gestores Públicos Estaduais no Brasil

PARTE I – DA ORGANIZAÇÃO

1. Razão Social _____ (preenchimento opcional)

2. Tipo da Organização
( ) administração direta ( ) autarquia ( ) economia mista ( ) agência
( ) outros. Qual? _____

3. Setor de atuação da Organização
( ) TI ( ) gestão ( ) planejamento

4. Unidade da Federação: _____

5. Parque de informática: _____ número **estimado** de estações de trabalho (micros em rede) – informar "0" se não tiver condições de estimar

6. Número **estimado** de usuários que acessam a rede: _____ (informar "0" se não tiver condições de estimar)

7. Esta organização já sofreu algum ataque (de hacker, por exemplo)?
( ) nunca sofreu ( ) já sofreu ( ) não sei ( ) não posso responder

8. O setor que é responsável pela Segurança da Informação (SI) desta organização está vinculado diretamente ao:
( ) Titular da Organização ( ) Segundo escalão ( ) Não existe setor formal para tratar de SI
( ) desconheço

PARTE II – DO RESPONDENTE

9. Área de atuação do respondente
( ) gestão de TI ( ) gestão de projeto (planejamento e gestão)

10. Idade: _____

11. Sexo: ( ) masculino ( ) feminino

12. Nível de Escolaridade
( ) Segundo grau ( ) Nível superior incompleto ( ) Nível superior completo
( ) Nível superior com especialização ou MBA ( ) Nível superior com Mestrado ou Doutorado
( ) outros. Especificar: _____

13. Conhecimento geral em informática:
( ) nenhum conhecimento
( ) noções básicas (Windows, editor de texto, acesso a internet)
( ) conhecimentos intermediários (básicos + planilha eletrônica e/ou software de apresentação)
( ) conhecimento avançados (intermediários + programar bancos de dados e/ou criar home-pages)

14. Treinamento em rede e/ou segurança da informação:
( ) nenhum conhecimento
( ) noções básicas (até 40 horas de curso)
( ) conhecimentos intermediários (de 40 a 80 horas de curso)
( ) conhecimento avançados (mais de 80 horas de curso)

15. Seu papel na adoção de novas tecnologias na sua organização é de:
( ) apenas usuário ( ) definição de especificações ( ) autorização de adoção

16. Você costuma usar a rede do trabalho para acessar contas pessoais:
( ) sempre ( ) às vezes ( ) nunca

17. Você costuma fazer back up de seus arquivos com que freqüência:
( ) diariamente ( ) quinzenalmente ( ) mensalmente ( ) intervalos maiores que um mês ( ) nunca

PARTE III					
(1) discordo totalmente (2) discordo (3) não concordo, nem discordo (4) concordo (5) concordo totalmente					
MARQUE COM "X" DE ACORDO COM SEU NÍVEL DE CONCORDÂNCIA	**1**	**2**	**3**	**4**	**5**
18. A utilização de práticas de Segurança da Informação requer muito do meu esforço mental					
19. Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação					
20. Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente					
21. A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho					
22. Eu gosto de utilizar práticas avançadas de Segurança da Informação					
23. Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante					
(1) altamente improvável (2) improvável (3) não sei (4) provável (5) altamente provável					
MARQUE COM "X" DE ACORDO COM SEU NÍVEL DE CONCORDÂNCIA	**1**	**2**	**3**	**4**	**5**
24. Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las.					
25 Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria.					

PARTE IV					
(1) discordo totalmente (2) discordo (3) não concordo, nem discordo (4) concordo (5) concordo totalmente					
MARQUE COM "X" DE ACORDO COM SEU NÍVEL DE CONCORDÂNCIA	**1**	**2**	**3**	**4**	**5**
(1) Cada identificador de acesso da rede (ou login) deve ser único para cada usuário					
(2) A rede não deve aceitar login de usuários que estão de férias					
(3) Os usuários da rede devem se comprometer, por escrito, a manter sigilo de suas senhas					
(4) A reativação de senhas (para usuários que se esqueceram da senha) deve ser feita após identificação rigorosa de que é o próprio usuário quem está requerendo a reativação					
(5) Os direitos de acesso à rede devem ser revisados regularmente					
(6) Os usuários devem ser alertados a evitar registrar senhas em papel					
(7) Os usuários devem ser obrigados a alterar suas senhas em intervalos regulares de tempo					
(8) A entrada de senhas deve ser efetuada através do uso do mouse (teclado virtual)					
(9) O procedimento de entrada na rede (ou login) deve ser limitado a três tentativas					
(10) O sistema de gerenciamento de senhas deve proibir reutilização de senhas					
(11) Devem existir cuidados especiais para utilização de recursos de computação móvel (ex: notebooks)					
(12) Quando um usuário é desligado da organização, seus direitos de acesso devem ser imediatamente removidos					
(13) Deve existir controle de acesso físico por biometria na área de utilização da rede					
(14) Devem existir mecanismos de monitoramento/gravação de imagens das instalações físicas onde os equipamentos de controle da rede funcionam					
(15) Devem existir regras claras de responsabilização de má utilização dos recursos da rede					
(16) Deve existir alguma verificação do passado do pretenso usuário da rede para verificar se ele já infringiu alguma norma de segurança em empregos anteriores					
(17) Os novos usuários da rede devem assinar algum documento tomando ciência de suas responsabilidades para segurança das informações que utilizará no seu trabalho					
(18) Todos os usuários da rede devem receber treinamento adequado para as suas respectivas funções sobre suas responsabilidades na segurança das informações					
(19) Os usuários que cometem erros através de falhas de segurança devem ser formalmente responsabilizados através de processos disciplinares					
(20) Deve existir um procedimento formal para criação de um novo usuário na rede e registro de seu nível de acesso					

Apêndice B – Questionário aplicado com Gestores da ABEP

Nº

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS - DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO

FATORES QUE INFLUENCIAM A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO: Um Estudo com Gestores Públicos Estaduais no Brasil

PARTE I – DA ORGANIZAÇÃO

1. Razão Social _____ (preenchimento opcional)

2. Tipo da Organização
( ) administração direta ( ) autarquia ( ) economia mista ( ) agência
( ) outros. Qual? _____

3. Setor de atuação da Organização
( ) TI ( ) gestão ( ) planejamento

4. Unidade da Federação: _____

5. Parque de informática: _____ número **estimado** de estações de trabalho (micros em rede) – informar "0" se não tiver condições de estimar

6. Número **estimado** de usuários que acessam a rede: _____ (informar "0" se não tiver condições de estimar)

7. Esta organização já sofreu algum ataque (de hacker, por exemplo)?
( ) nunca sofreu ( ) já sofreu ( ) não sei ( ) não posso responder

8. O setor que é responsável pela Segurança da Informação (SI) desta organização está vinculado diretamente ao:
( ) Titular da Organização ( ) Segundo escalão ( ) Não existe setor formal para tratar de SI
( ) desconheço

PARTE II – DO RESPONDENTE

9. Área de atuação do respondente
( ) gestão de TI ( ) gestão de projeto (planejamento e gestão)

10. Idade: _____

11. Sexo: ( ) masculino ( ) feminino

12. Nível de Escolaridade
( ) Segundo grau ( ) Nível superior incompleto ( ) Nível superior completo
( ) Nível superior com especialização ou MBA ( ) Nível superior com Mestrado ou Doutorado
( ) outros. Especificar: _____

13. Conhecimento geral em informática:
( ) nenhum conhecimento
( ) noções básicas (Windows, editor de texto, acesso a internet)
( ) conhecimentos intermediários (básicos + planilha eletrônica e/ou software de apresentação)
( ) conhecimento avançados (intermediários + programar bancos de dados e/ou criar home-pages)

14. Treinamento em rede e/ou segurança da informação:
( ) nenhum conhecimento
( ) noções básicas (até 40 horas de curso)
( ) conhecimentos intermediários (de 40 a 80 horas de curso)
( ) conhecimento avançados (mais de 80 horas de curso)

15. Seu papel na adoção de novas tecnologias na sua organização é de:
( ) apenas usuário ( ) definição de especificações ( ) autorização de adoção

16. Você costuma usar a rede do trabalho para acessar contas pessoais:
( ) sempre ( ) às vezes ( ) nunca

17. Você costuma fazer back up de seus arquivos com que freqüência:
( ) diariamente ( ) quinzenalmente ( ) mensalmente ( ) intervalos maiores que um mês ( ) nunca

PARTE III

(1) discordo totalmente (2) discordo (3) não concordo, nem discordo (4) concordo (5) concordo totalmente

MARQUE COM "X" DE ACORDO COM SEU NÍVEL DE CONCORDÂNCIA	1	2	3	4	5
18. A utilização de práticas de Segurança da Informação requer muito do meu esforço mental					
19. Eu tenho muita facilidade em utilizar práticas avançadas de Segurança da Informação					
20. Adotar práticas de Segurança da Informação torna meu trabalho mais eficiente					
21. A utilização de práticas de Segurança da Informação é extremamente importante para a realização do meu trabalho					
22. Eu gosto de utilizar práticas avançadas de Segurança da Informação					
23. Utilizar práticas avançadas de Segurança da Informação torna meu trabalho mais interessante					

(1) altamente improvável (2) improvável (3) não sei (4) provável (5) altamente provável

MARQUE COM "X" DE ACORDO COM SEU NÍVEL DE CONCORDÂNCIA	1	2	3	4	5
24. Se eu tiver acesso às normas das práticas avançadas de Segurança da Informação, pretendo usá-las.					
25 Dado que eu tenha acesso às normas avançadas de Segurança da Informação, prevejo que as usaria.					

PARTE IV

(1) não implantado (2) em análise (3) em implantação (4) implantado parcialmente (5) implantado e disseminado (0) desconheço

MARQUE COM "X" A SITUAÇÃO MAIS PRÓXIMA DA SUA ORGANIZAÇÃO	1	2	3	4	5	0
(1) Cada identificador de acesso da rede (ou login) é único para cada usuário						
(2) A rede não aceita login de usuários que estão de férias						
(3) Os usuários da rede se comprometem, por escrito, a manter sigilo de suas senhas						
(4) A reativação de senhas (para usuários que se esqueceram da senha) é feita após identificação rigorosa de que é o próprio usuário quem está requerendo a reativação						
(5) Os direitos de acesso à rede são revisados regularmente						
(6) Os usuários são alertados a evitar registrar senhas em papel						
(7) Os usuários são obrigados a alterar suas senhas em intervalos regulares de tempo						
(8) A entrada de senhas é efetuada através do uso do mouse						
(9) O procedimento de entrada na rede (ou login) se limita a três tentativas						
(10) O sistema de gerenciamento de senhas proíbe reutilização de senhas						
(11) Existem cuidados especiais para utilização de recursos de computação móvel (ex: notebooks)						
(12) Quando um usuário é desligado da organização, seus direitos de acesso são imediatamente removidos						
(13) Existe controle de acesso físico por biometria na área de utilização da rede						
(14) Existem mecanismos de monitoramento/gravação de imagens das instalações físicas onde os equipamentos de controle da rede funcionam						
(15) Existem regras claras de responsabilização de má utilização dos recursos da rede						
(16) Existe alguma verificação do passado do pretenso usuário da rede para verificar se ele já infringiu alguma norma de segurança em empregos anteriores						
(17) Os novos usuários da rede assinam algum documento tomando ciência de suas responsabilidades para segurança das informações que utilizará no seu trabalho						
(18) Todos os usuários da rede recebem treinamento adequado para as suas respectivas funções sobre suas responsabilidades na segurança das informações						
(19) Os usuários que cometem erros através de falhas de segurança são formalmente responsabilizados através de processos disciplinares						
(20) Existe um procedimento formal para criação de um novo usuário na rede e registro de seu nível de acesso						

Apêndice C – Controle de Entrega dos Questionários do PNAGE

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS - DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO
FATORES QUE INFLUENCIAM A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO: Um Estudo com Gestores Públicos Estaduais no Brasil

CONTROLE DE ENTREGA DE QUESTIONÁRIOS PNAGE

Nº	UF	ENTREGUE	DEVOLVIDO
101	AC	pessoalmente	pessoalmente
102	AC	enviado por membro da UCE/PNAGE	por fax
103	AL	pessoalmente	pessoalmente
104	AL	pessoalmente	pessoalmente
105	AL	pessoalmente	pessoalmente
106	AL	pessoalmente	pessoalmente
107	AM	pessoalmente	pessoalmente
108	AM	enviado por membro da UCE/PNAGE	por email
109	AM	enviado por membro da UCE/PNAGE	por email
110	AM	enviado por membro da UCE/PNAGE	por email
111	AP	pessoalmente	por email
112	AP	pessoalmente	por email
113	AP	enviado por membro da UCE/PNAGE	por emial
114	AP	enviado por membro da UCE/PNAGE	por email
115	BA	pessoalmente	pessoalmente
116	BA	pessoalmente	pessoalmente
117	BA	enviado por membro da UCE/PNAGE	por email
118	BA	enviado por membro da UCE/PNAGE	por email
119	CE	pessoalmente	pessoalmente
120	CE	pessoalmente	pessoalmente
121	CE	pessoalmente	pessoalmente
122	CE	pessoalmente	pessoalmente
123	DF	pessoalmente	por email
124	DF	enviado por membro da UCE/PNAGE	por email
125	DF	enviado por membro da UCE/PNAGE	por email
126	DF	enviado por membro da UCE/PNAGE	por email
127	ES	pessoalmente	por email
128	ES	pessoalmente	por email
129	ES	enviado por membro da UCE/PNAGE	por email
130	MA	pessoalmente	pessoalmente
131	MA	enviado por membro da UCE/PNAGE	por email
132	MA	enviado por membro da UCE/PNAGE	
133	MA	enviado por membro da UCE/PNAGE	
134	MG	enviado por membro da UCE/PNAGE	por email
135	MG	enviado por membro da UCE/PNAGE	por email
136	MG	enviado por membro da UCE/PNAGE	por email
137	MG	pessoalmente	pessoalmente

138	MS	pessoalmente	pessoalmente
139	MS	enviado por membro da UCE/PNAGE	
140	PA	pessoalmente	pessoalmente
141	PA	enviado por membro da UCE/PNAGE	
142	PA	enviado por membro da UCE/PNAGE	por fax
143	PB	pessoalmente	por fax
144	PB	enviado por membro da UCE/PNAGE	por fax
145	PB	enviado por membro da UCE/PNAGE	por fax
146	PB	enviado por membro da UCE/PNAGE	
147	PB	enviado por membro da UCE/PNAGE	por fax
148	PE	pessoalmente	pessoalmente
149	PE	pessoalmente	pessoalmente
150	PE	pessoalmente	pessoalmente
151	PI	enviado por membro da UCE/PNAGE	
152	PI	enviado por membro da UCE/PNAGE	
153	PI	pessoalmente	pessoalmente
154	PI	pessoalmente	pessoalmente
155	PR	pessoalmente	pessoalmente
156	PR	pessoalmente	pessoalmente
157	PR	enviado por membro da UCE/PNAGE	por email
158	RJ	pessoalmente	pessoalmente
159	RJ	pessoalmente	pessoalmente
160	RJ	pessoalmente	pessoalmente
161	RJ	pessoalmente	pessoalmente
162	RN	pessoalmente	pessoalmente
163	RN	pessoalmente	pessoalmente
164	RN	pessoalmente	pessoalmente
165	RO	por email	por email
166	RO	por email	
167	RO	por email	
168	RO	por email	
169	RR	por email	por email
170	RR	por email	por email
171	RR	por email	por email
172	RR	por email	
173	RS	pessoalmente	por fax
174	RS	enviado por membro da UCE/PNAGE	por fax
175	RS	enviado por membro da UCE/PNAGE	por fax
176	RS	enviado por membro da UCE/PNAGE	por fax
177	RS	enviado por membro da UCE/PNAGE	
178	SC	pessoalmente	pessoalmente
179	SC	pessoalmente	pessoalmente
180	SC	enviado por membro da UCE/PNAGE	por fax
181	SC	enviado por membro da UCE/PNAGE	
182	SE	pessoalmente	pessoalmente
183	SE	pessoalmente	pessoalmente

184	SE	enviado por membro da UCE/PNAGE	
185	SE	enviado por membro da UCE/PNAGE	por email
186	SE	enviado por membro da UCE/PNAGE	por email
187	SP	pessoalmente	pessoalmente
188	SP	pessoalmente	pessoalmente
189	SP	enviado por membro da UCE/PNAGE	
190	SP	enviado por membro da UCE/PNAGE	
191	TO	pessoalmente	pessoalmente
192	TO	pessoalmente	pessoalmente
193	TO	pessoalmente	pessoalmente
194	TO	pessoalmente	pessoalmente
195	MT	pessoalmente	pessoalmente
196	AC	enviado por membro da UCE/PNAGE	por fax
197	AC	enviado por membro da UCE/PNAGE	

Apêndice D – Controle de Entrega dos Questionários do ABEP

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS - DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO
FATORES QUE INFLUENCIAM A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO: Um Estudo com Gestores Públicos Estaduais no Brasil

CONTROLE DE ENTREGA DE QUESTIONÁRIOS ABEP

Nº	UF	ENTREGUE	DEVOLVIDO
001	AC	pessoalmente	pessoalmente
002	AC	enviado por José Alcimar (UCE/PNAGE)	por fax
003	AC	enviado por José Alcimar (UCE/PNAGE)	por fax
004	AC	enviado por José Alcimar (UCE/PNAGE)	por fax
005	AL	enviado por Adelmo (UCE/PNAGE)	
006	AL	enviado por Adelmo (UCE/PNAGE)	
007	AL	enviado por Adelmo (UCE/PNAGE)	
008	AL	enviado por Adelmo (UCE/PNAGE)	
009	AL	enviado por Adelmo (UCE/PNAGE)	
010	AM	enviado por César (UCE/PNAGE)	por email
011	AM	enviado por César (UCE/PNAGE)	por email
012	AM	enviado por César (UCE/PNAGE)	por email
013	AP	enviado por Oneide (UCE/PNAGE)	
014	AP	enviado por Oneide (UCE/PNAGE)	
015	AP	enviado por Oneide (UCE/PNAGE)	
016	AP	enviado por Oneide (UCE/PNAGE)	
017	AP	enviado por Oneide (UCE/PNAGE)	
018	BA	enviado por Luciane (UCE/PNAGE)	por email
019	BA	enviado por Luciane (UCE/PNAGE)	por email
020	BA	enviado por Luciane (UCE/PNAGE)	por email
021	BA	enviado por Luciane (UCE/PNAGE)	por email
022	BA	enviado por Luciane (UCE/PNAGE)	por email
023	CE	enviado por Lucia (UCE/PNAGE)	por email
024	CE	enviado por Lucia (UCE/PNAGE)	
025	CE	enviado por Lucia (UCE/PNAGE)	
026	CE	enviado por Lucia (UCE/PNAGE)	
027	ES	enviado por Verônica (UCE/PNAGE)	por terceiros
028	ES	enviado por Verônica (UCE/PNAGE)	por terceiros
029	ES	enviado por Verônica (UCE/PNAGE)	por terceiros
030	GO	enviado por Luciano (COTIC/SEARH)	
031	GO	enviado por Luciano (COTIC/SEARH)	
032	MA	enviado por Domingos (UCE/PNAGE)	
033	MA	enviado por Domingos (UCE/PNAGE)	
034	MA	enviado por Domingos (UCE/PNAGE)	
035	MA	enviado por Domingos (UCE/PNAGE)	
036	MA	enviado por Domingos (UCE/PNAGE)	

037	MG	enviado por Luciene (UCE/PNAGE)	
038	MG	enviado por Luciene (UCE/PNAGE)	
039	MG	enviado por Luciene (UCE/PNAGE)	
040	MG	enviado por Luciene (UCE/PNAGE)	
041	MG	enviado por Luciene (UCE/PNAGE)	
042	MG	enviado por Luciene (UCE/PNAGE)	
043	MS	enviado por Ilton (UCE/PNAGE)	
044	MS	enviado por Ilton (UCE/PNAGE)	
045	MS	enviado por Ilton (UCE/PNAGE)	
046	MT	enviado por Juracy (UCE/PNAGE)	
047	MT	enviado por Juracy (UCE/PNAGE)	
048	MT	enviado por Juracy (UCE/PNAGE)	
049	MT	enviado por Juracy (UCE/PNAGE)	
050	PA	enviado por Edilena (UCE/PNAGE)	por fax
051	PA	enviado por Edilena (UCE/PNAGE)	por fax
052	PA	enviado por Edilena (UCE/PNAGE)	por fax
053	PA	enviado por Edilena (UCE/PNAGE)	por fax
054	PA	enviado por Edilena (UCE/PNAGE)	
055	PB	enviado por João Manuel (UCE/PNAGE)	pelo correio
056	PB	enviado por João Manuel (UCE/PNAGE)	pelo correio
057	PB	enviado por João Manuel (UCE/PNAGE)	pelo correio
058	PE	enviado por Analúcia (UCE/PNAGE)	Por email
059	PE	enviado por Analúcia (UCE/PNAGE)	
060	PE	enviado por Analúcia (UCE/PNAGE)	
061	PI	enviado por Raimundo (UCE/PNAGE)	
062	PI	enviado por Raimundo (UCE/PNAGE)	
063	PI	enviado por Raimundo (UCE/PNAGE)	
064	PR	enviado por Conchita (UCE/PNAGE)	por email
065	PR	enviado por Conchita (UCE/PNAGE)	
066	PR	enviado por Conchita (UCE/PNAGE)	por email
067	PR	enviado por Conchita (UCE/PNAGE)	
068	PR	enviado por Conchita (UCE/PNAGE)	por email
069	RJ	enviado por Stella (UCE/PNAGE)	
070	RJ	enviado por Stella (UCE/PNAGE)	
071	RJ	enviado por Stella (UCE/PNAGE)	
072	RJ	enviado por Stella (UCE/PNAGE)	
073	RJ	enviado por Stella (UCE/PNAGE)	
074	RJ	enviado por Stella (UCE/PNAGE)	
075	RJ	enviado por Stella (UCE/PNAGE)	
076	RN	pessoalmente	pessoalmente
077	RN	pessoalmente	pessoalmente
078	RN	pessoalmente	pessoalmente
079	RN	pessoalmente	pessoalmente
080	RR	enviado por Lucinete (UCE/PNAGE)	por email
081	RR	enviado por Lucinete (UCE/PNAGE)	
082	RR	enviado por Lucinete (UCE/PNAGE)	

083	RR	enviado por Lucinete (UCE/PNAGE)	
084	RS	enviado por Lisandra (UCE/PNAGE)	por email
085	RS	enviado por Lisandra (UCE/PNAGE)	
086	RS	enviado por Lisandra (UCE/PNAGE)	
087	RS	enviado por Lisandra (UCE/PNAGE)	
088	SC	enviado por Silvana (UCE/PNAGE)	por email
089	SC	enviado por Silvana (UCE/PNAGE)	
090	SC	enviado por Silvana (UCE/PNAGE)	
091	SC	enviado por Silvana (UCE/PNAGE)	
092	SE	enviado por Andrea (UCE/PNAGE)	por email
093	SE	enviado por Andrea (UCE/PNAGE)	por fax
094	SE	enviado por Andrea (UCE/PNAGE)	
095	SP	enviado por Mário Sérgio (UCE/PNAGE)	
096	SP	enviado por Mário Sérgio (UCE/PNAGE)	
097	SP	enviado por Mário Sérgio (UCE/PNAGE)	
098	SP	enviado por Mário Sérgio (UCE/PNAGE)	
099	SP	enviado por Mário Sérgio (UCE/PNAGE)	
100	TO	enviado por Ribamar (UCE/PNAGE)	por fax

Apêndice E – Alterações da Norma ISO 27001:2005 em relação às normas anteriores

Em relação aos padrões anteriores, dos capítulos da norma destaca-se que a parte introdutória não possui nenhuma alteração significativa. A ISO 27001:2005 ainda possui uma introdução semelhante à BS 7799-2:2002. A referência ao processo de abordagem ainda foi mantida, mas com uma maior elaboração. Há também a importante ressalva de que essa norma está alinhada com a ISO 9001:2000 e ISO 14001:2004 e que ela foi projetada para permitir a qualquer organização alinhar ou integrar seu SGSI relacionado com os requisitos do sistema de gestão.

A **Cláusula 1** define o **escopo**, informando que esta norma é aplicável a todas as organizações. A **Cláusula 2** estabelece **Referências Normativas,** mostrando que a ISO 270001:2005 está diretamente relacionada com a norma ISO / IEC 17799:2005 para a sua aplicação. A **Cláusula 3** apresenta **Termos e Definições,** sendo que alguns foram adicionados e outros modificados ou substituídos para alinhar com outras normas, tais como ISO / IEC 13335-1:2004 e ISO / IEC 18044:2004 TR. Além de algumas das definições foram modificadas e esclarecidas.

A **Cláusula 4** trata de diversos conceitos relacionados a Sistemas de Gestão de Segurança da informação – **SGSI**. A **cláusula 4.1** (**Requisitos Gerais)** foi uma exigência esclarecida a fim de incluir as atividades de operação, controle e fiscalização da Documentação dos SGSI.

A Cláusula 4.2 (**Estabelecer e Acompanhamento do SGSI)** é composta de quatro itens e as suas alterações são listadas a seguir:

Na subcláusula 4.2.1 - Estabelecer o SGSI:

a) Definir o escopo de aplicação: este requisito foi modificado para garantir que também seja delimitado o SGSI. A necessidade de limites sempre foi anteriormente implícita, mas agora ele está claramente expressa e deve incluir detalhes e justificativa para qualquer exclusões.

b) Definir a política SGSI: modificado para garantir alinhamento com a estratégia organizacional do contexto da gestão de risco contexto. Há uma nota indicativa de que o SGSI é um subconjunto de Política de Segurança da Informação.

c) Definir a abordagem de avaliação dos riscos da organização: o texto deste tópico foi reestruturado para proporcionar uma lista discriminada. Consta uma

Nota que faz referência a exemplos de metodologias de avaliação de riscos encontrados na norma ISO/IEC TR 13335-3.

d) Identificar os riscos: texto inalterado, mas nota acrescentado o termo "proprietário de ativos”.

e) Analisar e avaliar os riscos (anteriormente era "avaliar os riscos"): ligeiras modificações com expressões como "mal negócio" agora substituídos com "impacto sobre o negócio da organização".

g) Selecionar objetivos de controle: texto expandido para esclarecer que a seleção e implementação de objetivos de controle e controles deve satisfazer as necessidades identificadas que foram identificadas pela avaliação de risco e tratamento. Acrescentou nota explicativa sobre conteúdo e finalidade do Anexo A.

h) Obter aprovação da gestão: reestruturada.

i) Autorizar implementar e operar o SGSI: reestruturada.

j) Preparar uma Declaração de Aplicabilidade: texto existente reformulado em uma lista discriminada para esclarecer que a Declaração de Aplicabilidade incluirá os atuais objetivos de controle e respectivos controles. Acrescentou que a Declaração de Aplicabilidade fornece um resumo das decisões de risco relativo e justifica exclusões.

Na subcláusula 4.2.2 - Implementar e operar o SGSI:

a) Formular um plano de tratamento de risco: "recursos" adicionado à lista de medidas de gestão adequadas.

d) Definir a forma de medida: para complementar os requisitos necessários para implementar e utilizar o SGSI é necessário definir a forma de medir a eficácia dos controles ou grupos de controle e também como estas medidas devem ser utilizados para avaliar a eficácia de controle para produzir e comparar resultados.

f) Gerir as operações: SGSI acrescentado para prestar esclarecimentos sobre as operações são geridas.

g) Gerir recursos: SGSI acrescentado para prestar esclarecimentos sobre quais recursos são geridos.

Na subcláusula 4.2.3 - Supervisão e revisão do SGSI:

a) Executar os procedimentos de controle: Requer que a execução possua acompanhamento contínuo, mas apenas nesta versão da norma inclui a revisão dos procedimentos. Na subcláusula 2, foi incluída a palavra "tentativa" de

modo a garantir que todas as violações e incidentes estão incluídos. Na subcláusula 4 houve a inclusão do termo detecção de eventos de segurança e, assim, impedir segurança incidentes com o uso de indicadores. A subcláusula 5 foi modificada para garantir que as medidas tomadas para resolver uma violação de segurança sejam eficazes.

b) Realizar exames regulares: este requisito foi modificado para incluir os resultados de eficácia de medições nas revisões periódicas.

c) Medir a eficácia dos controles: além da obrigatoriedade anterior em acompanhar e revisar o SGSI, é necessário medir a eficácia dos controles para verificar se os requisitos de segurança foram atendidos.

d) Rever as avaliações de riscos: texto modificado para incluir o exame de avaliação dos riscos sejam realizados em intervalos planejados. A subcláusula d.5 é um complemento à exigência de incluir a eficácia dos controles implementados no âmbito da revisão. Na subcláusula d.6, a expressão "mudou as obrigações contratuais" foi adicionada.

e) Realizar auditorias internas no SGSI: não foi alterado o texto, mas a referência dada ao título foi renovada. Acrescentou nota explicando quem deve realizar auditorias internas.

f) Realizar uma revisão gerencial: foi suprimida a periodicidade de pelo menos uma vez por ano.

g) Atualização de segurança planos: nova exigência.

Na subcláusula 4.2.4 - Manter e melhorar o SGSI:

c) Comunicar as ações e melhorias: texto alterado para garantir que haja um nível de detalhe adequado para circunstâncias e, conforme o caso, como proceder.

A Cláusula 4.3 (**Documentação)** é dividida em três partes e suas alterações em relação à norma anterior são apresentadas a seguir:

Na subcláusula 4.3.1 - Geral: Novos parágrafos introdutórios explicam detalhadamente o que é esperado em termos de documentação. Também é feita a inclusão dos registros das decisões de gestão.

a) Documentação de declarações: revista para abordar Política de SGSI.

b) Escopo do SGSI: suprime a referência a "procedimentos e controles”, em apoio do SGSI.

c) Insere a referência a "procedimentos e controles, em apoio do SGSI".

d) Descrição da metodologia de análise de riscos: esclarece, garantindo que a descrição da a metodologia de análise de riscos é incluída dentro da documentação.

g) Documentação de Procedimentos: texto expandido para descrever como medir a eficácia dos controles.

Na subcláusula 4.3.2 - Controle de Documentos:

d) Assegurar as versões: mudou de "versões mais recentes de documentos relevantes" para "Versões relevantes dos documentos aplicáveis".

f) Assegurar que os documentos estão disponíveis: esclarecido para garantir que os documentos estão disponíveis para aqueles que deles necessitam, e que são transferidos, armazenados e, finalmente, eliminados de acordo com o procedimentos aplicáveis à sua classificação.

Na subcláusula 4.3.3 - Controle de registros:

No primeiro parágrafo, a segunda frase foi alterada para "Eles devem ser protegidos e controlados ". A terceira frase foi ampliada para abranger também "dos requisitos regulamentares e contratuais e obrigações". A quinta frase foi ampliada para exigir que os controles devem ser "documentados e implementados". A última frase deste requisito em BS 7799-2:2002 foi suprimida. No segundo parágrafo, a palavra "significativa" foi adicionada à frente de incidentes de segurança ".

A **Cláusula 5** trata da **Gestão de Responsabilidade. A cláusula 5.1 (compromisso de gestão)** teve as seguintes alterações:

a) Estabelecer um SGSI: a expressão "política de segurança da informação" foi substituída por "Política de SGSI ", destacando como foco principal o SGSI.

b) Assegurar SGSI: a expressão "objetivos da segurança da informação" foi substituída por " objetivos do SGSI", destacando como foco principal o SGSI.

e) Disponibilizar recursos suficientes: a descrição das atividades SGSI foi alinhado com a definição do SGSI.

f) Decidir os critérios: Esta exigência foi expandida para cobrir a decisão sobre "critérios de aceitação de riscos e níveis de risco aceitável ".

g) Assegurar auditorias internas: Este é um esclarecimento, para além do compromisso com a gestão garantir que sejam realizadas auditorias internas SGSI. Inclui uma referência ao novo artigo 6.

Já a **cláusula 5.2 (Gestão de Recursos)** sofreu os seguintes ajustes:

Na subcláusula 5.2.1 - Provisão de Recursos:

a) Estabelecer, implementar, operar: texto ampliado para cobrir toda a gama de atividades relacionadas a um SGSI.

Na subcláusula 5.2.2 - Formação de sensibilização e competência:

b) Proporcionar formação: texto foi alterado para ter em conta a possibilidade de tomar outras medidas. Esta mudança foi feita para alinhar com a norma ISO 9001:2000.

c) Avaliação da eficácia: o mesmo foi reduzido para "avaliar a eficácia das ações tomadas".

A Cláusula 6 trata de **Auditorias internas do SGSI.** Da anterior **subcláusula 6.4** para BS 7799-2:2002 foi feita uma primeira cláusula na norma ISO 27001:2005 e o texto foi transferido na totalidade, com os ajustes a seguir:

- Quarto parágrafo: na segunda frase, a expressão "melhoria das atividades" foi substituída por "atividades de acompanhamento".
- Uma nova nota foi adicionado ao referir-se à norma ISO 19011:2002 Diretrizes para a qualidade e/ou questão ambiental em sistemas de gestão de auditoria.

A **Cláusula 7** foca na **revisão da gestão do SGSI.** A numeração da cláusula foi ajustada para inserção do novo artigo 6. Em **7.1 (Geral)** há mudança de numeração e pequena alteração no primeiro parágrafo. Além disso, o texto modificado em que "a política de segurança e de objetivos de segurança" foi substituída por "Política Segurança da informação e os objetivos de Segurança da Informação", a fim de esclarecer o que foi incluído na revisão.

Na **revisão de entrada (cláusula 7.2)** há mudança de numeração e pequena mudança. Já na **revisão de saída (cláusula 7.3)** ocorreu mudança de numeração e os seguintes ajustes:

b) Atualização do risco - a clarificação e expansão de texto para atualizar a avaliação do risco e de risco plano de tratamento.

c) Modificações de procedimentos: o texto foi ampliado para incluir as "alterações de procedimentos e controles" e seis níveis de risco.

e) Melhorias a fazer: texto tornou-se mais claro.

A Cláusula 8 refere-se à **Melhoria do SGSI.** Ela teve a numeração ajustada devido à introdução da nova cláusula 6 e alguns ajustes nos seus detalhamentos. A cláusula **8.1 (melhoria contínua)** teve a palavra “informação” incluída no Primeiro parágrafo na frente de "objetivos de segurança". Já cláusula **8.2 (ação corretiva)** teve a numeração ajustada e o texto relativo à "associados com a implementação e operação do SGSI "substituído por "com

os requisitos do SGSI" e no item “a” o texto foi abreviado. Em **8.3 (ação preventiva)** a numeração foi ajustada e o texto foi adaptado de "proteger contra futuras desconformidades" para "com os requisitos do SGSI" e o item “b” foi alterado para exigir que a organização identifique os riscos e identifique as ações preventivas, centrando sua atenção sobre requisitos dos riscos.

Já às alterações dos anexos da norma ISO/IEC 27001 em relação às anteriores, percebe-se que **o Anexo A** foi atualizado, mas correspondem às orientações da norma ISO/IEC 17799: 2005. O **Anexo B** teve alterações com redução do texto. O **Anexo C** foi reestruturado de forma a corresponder com a norma ISO 9001:2000 e o **Anexo D** foi removido.

Apêndice F – Tabelas de Resultados em relação à Organização

Tabela 87 – Distribuição de freqüências do Tipo da Organização

Tipo da organização	Freq	%
Administração Direta	79	98,75
Outros	1	1,25
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 88 – Distribuição de freqüências do setor de atuação

Setor de atuação	Freq	%
Gestão	37	46,84
Planejamento	25	31,65
Gestão e Planejamento	12	15,19
TI e Gestão	2	2,53
TI	2	2,53
TI, Gestão e Planejamento	1	1,27
Total	79	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 89 – Distribuição de freqüências de Incidência de ataque

Incidência de ataques	Freq	%
Não sei	39	50,65
Já sofreu	22	28,57
Nunca sofreu	10	12,99
Não posso responder	6	7,79
Total	77	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 90 – Distribuição de freqüências do setor responsável pela segurança

Setor responsável pela segurança da Informação (SI)	Freq	%
Titular da organização	36	46,15
Segundo escalão	28	35,90
Desconheço	8	10,26
Não existe setor formal	6	7,69
Total	78	100,00

Fonte: Resultados da pesquisa (2009)

Apêndice G – Tabelas de Resultados em relação ao Respondente

Tabela 91 – Distribuição de freqüências de área de atuação

Área de atuação	Freq	%
Gestão de projeto	78	97,50
Gestão de TI	2	2,50
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 92 – Distribuição de freqüências do sexo

Sexo	Freq	%
Masculino	45	56,25
Feminino	35	43,75
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 93 – Distribuição de freqüências do Nível de escolaridade

Escolaridade	Freq	%
2o. grau	2	2,50
Superior incompleto	2	2,50
Superior completo	20	25,00
Especialista	48	60,00
Mestrado ou doutorado	8	10,00
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 94 – Distribuição de freqüências do Conhecimento geral em informática

Conhecimento em informática	Freq	%
Noções básicas	20	25,00
Intermediário	47	58,75
Avançado	13	16,25
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 95 – Distribuição de freqüências do Treinamento em rede e/ou segurança da informação

Treinamento em rede ou segurança	Freq	%
Nenhum conhecimento	39	49,37
Noções básicas	25	31,65
Intermediário	11	13,92
Avançado	4	5,06
Total	79	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 96 – Distribuição de freqüências do papel na adoção de novas tecnologias na sua organização é de

Papel na adoção de TI	Freq	%
Apenas usuário	61	76,25
Definição de especificações	15	18,75
Autorização de adoção	4	5,00
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 97 – Distribuição de freqüências do uso de rede do trabalho para acessar contas pessoais

Uso da rede para contas pessoais	Freq	%
Às vezes	41	51,25
Sempre	20	25,00
Nunca	19	23,75
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 98 – Distribuição de freqüências das vezes que costuma fazer back up de seus arquivos com que freqüência:

Frequência de backup	Freq	%
Diariamente	8	10,13
Quinzenalmente	6	7,59
Mensalmente	14	17,72
Mais que um mês	34	43,04
Nunca	17	21,52
Total	79	100,00

Fonte: Resultados da pesquisa (2009)

Apêndice H – Tabelas de Resultados em relação ao Modelo TAM

Tabela 99 – Respostas Modelo TAM - Facilidade de Utilização 1

Muito esforço mental	Freq	%
Discordo totalmente	17	21,25
Discordo parcialmente	25	31,25
Neutro	24	30,00
Concordo parcialmente	12	15,00
Concordo totalmente	2	2,50
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 100 – Respostas Modelo TAM - Facilidade de Utilização 2

Facilidade em utilizar	Freq	%
Discordo totalmente	9	11,25
Discordo parcialmente	19	23,75
Neutro	24	30,00
Concordo parcialmente	20	25,00
Concordo totalmente	8	10,00
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 101 – Percepções sobre a Utilidade 1

Torna trabalho mais eficiente	Freq	%
Discordo totalmente	4	5,00
Discordo parcialmente	7	8,75
Neutro	8	10,00
Concordo parcialmente	41	51,25
Concordo totalmente	20	25,00
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 102 - Percepções sobre a Utilidade 2

Importância para a realização do trabalho	Freq	%
Discordo totalmente	1	1,25
Discordo parcialmente	8	10,00
Neutro	15	18,75
Concordo parcialmente	37	46,25
Concordo totalmente	19	23,75
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 103 – Atitude 1

Gosto por utilizar	Freq	%
Discordo totalmente	3	3,75
Discordo parcialmente	10	12,50
Neutro	31	38,75
Concordo parcialmente	27	33,75
Concordo totalmente	9	11,25
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 104 – Atitude 2

Torna trabalho mais interessante	Freq	%
Discordo totalmente	3	3,75
Discordo parcialmente	13	16,25
Neutro	31	38,75
Concordo parcialmente	27	33,75
Concordo totalmente	6	7,50
Total	80	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 105 - Intenção de Utilização 1

Com acesso, vai usar	Freq	%
Improvável	1	1,27
Não sei	8	10,13
Provável	46	58,23
Altamente provável	24	30,38
Total	79	100,00

Fonte: Resultados da pesquisa (2009)

Tabela 106 - Intenção de Utilização 2

Previsão de uso	Freq	%
Improvável	2	2,53
Não sei	9	11,39
Provável	43	54,43
Altamente provável	25	31,65
Total	79	100,00

Fonte: Resultados da pesquisa (2009)

Apêndice I– Tabelas da Análise Fatorial

Tabela 107 – Matriz de correlação: Adoção de práticas avançadas de Segurança

		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20
Correlation	V1	1	0,17	0,28	0,61	0,35	0,34	0,39	0,24	0,24	0,07	0,20	0,40	0,40	0,44	0,35	0,26	0,44	0,45	0,25	0,62
	V2	0,17	1	0,16	0,13	0,25	0,25	0,33	0,22	0,34	0,29	0,32	0,28	0,15	0,36	0,37	0,19	0,30	0,34	0,27	0,31
	V3	0,28	0,16	1	0,38	0,44	0,38	0,37	0,29	0,32	0,20	0,23	0,08	0,33	0,16	0,28	0,41	0,50	0,39	0,28	0,44
	V4	0,61	0,13	0,38	1	0,38	0,53	0,36	0,30	0,36	0,28	0,29	0,18	0,44	0,51	0,41	0,28	0,41	0,43	0,30	0,53
	V5	0,35	0,25	0,44	0,38	1	0,48	0,42	0,35	0,25	0,26	0,42	0,38	0,34	0,27	0,28	0,35	0,44	0,41	0,39	0,42
	V6	0,34	0,25	0,38	0,53	0,48	1	0,35	0,47	0,46	0,39	0,34	0,29	0,26	0,42	0,23	0,31	0,52	0,56	0,34	0,49
	V7	0,39	0,33	0,37	0,36	0,42	0,35	1	0,38	0,20	0,48	0,28	0,11	0,23	0,37	0,20	0,40	0,34	0,36	0,29	0,44
	V8	0,24	0,22	0,29	0,30	0,35	0,47	0,38	1	0,35	0,37	0,13	0,07	0,01	0,23	0,03	0,34	0,30	0,35	0,16	0,32
	V9	0,24	0,34	0,32	0,36	0,25	0,46	0,20	0,35	1	0,42	0,20	0,10	0,39	0,24	0,06	0,27	0,24	0,23	0,32	0,33
	V10	0,07	0,29	0,20	0,28	0,26	0,39	0,48	0,37	0,42	1	0,24	0,08	0,13	0,21	-0,02	0,32	0,24	0,21	0,24	0,32
	V11	0,20	0,32	0,23	0,29	0,42	0,34	0,28	0,13	0,20	0,24	1	0,06	0,26	0,43	0,47	0,28	0,30	0,31	0,33	0,30
	V12	0,40	0,28	0,08	0,18	0,38	0,29	0,11	0,07	0,10	0,08	0,06	1	0,16	0,25	0,25	0,16	0,37	0,27	0,14	0,32
	V13	0,40	0,15	0,33	0,44	0,34	0,26	0,23	0,01	0,39	0,13	0,26	0,16	1	0,50	0,29	0,19	0,24	0,20	0,54	0,34
	V14	0,44	0,36	0,16	0,51	0,27	0,42	0,37	0,23	0,24	0,21	0,43	0,25	0,50	1	0,49	0,34	0,35	0,43	0,38	0,46
	V15	0,35	0,37	0,28	0,41	0,28	0,23	0,20	0,03	0,06	-0,02	0,47	0,25	0,29	0,49	1	0,27	0,47	0,45	0,32	0,49
	V16	0,26	0,19	0,41	0,28	0,35	0,31	0,40	0,34	0,27	0,32	0,28	0,16	0,19	0,34	0,27	1	0,52	0,38	0,23	0,28
	V17	0,44	0,30	0,50	0,41	0,44	0,52	0,34	0,30	0,24	0,24	0,30	0,37	0,24	0,35	0,47	0,52	1	0,66	0,31	0,53
	V18	0,45	0,34	0,39	0,43	0,41	0,56	0,36	0,35	0,23	0,21	0,31	0,27	0,20	0,43	0,45	0,38	0,66	1	0,41	0,56
	V19	0,25	0,27	0,28	0,30	0,39	0,34	0,29	0,16	0,32	0,24	0,33	0,14	0,54	0,38	0,32	0,23	0,31	0,41	1	0,31
	V20	0,62	0,31	0,44	0,53	0,42	0,49	0,44	0,32	0,33	0,32	0,30	0,32	0,34	0,46	0,49	0,28	0,53	0,56	0,31	1
Sig. (1-tailed)	V1		0,07	0,01	0,00	0,00	0,00	0,00	0,02	0,02	0,28	0,04	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,01	0,00
	V2	0,07		0,08	0,14	0,01	0,01	0,00	0,03	0,00	0,01	0,00	0,01	0,09	0,00	0,00	0,05	0,00	0,00	0,01	0,00
	V3	0,01	0,08		0,00	0,00	0,00	0,00	0,00	0,00	0,04	0,02	0,24	0,00	0,09	0,01	0,00	0,00	0,00	0,01	0,00
	V4	0,00	0,14	0,00		0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,06	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00
	V5	0,00	0,01	0,00	0,00		0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00
	V6	0,00	0,01	0,00	0,00	0,00		0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,02	0,00	0,00	0,00	0,00	0,00
	V7	0,00	0,00	0,00	0,00	0,00	0,00		0,00	0,04	0,00	0,01	0,17	0,02	0,00	0,04	0,00	0,00	0,00	0,01	0,00
	V8	0,02	0,03	0,00	0,00	0,00	0,00	0,00		0,00	0,00	0,14	0,27	0,46	0,02	0,41	0,00	0,00	0,00	0,08	0,00
	V9	0,02	0,00	0,00	0,00	0,01	0,00	0,04	0,00		0,00	0,04	0,19	0,00	0,02	0,30	0,01	0,02	0,02	0,00	0,00
	V10	0,28	0,01	0,04	0,01	0,01	0,00	0,00	0,00	0,00		0,02	0,26	0,13	0,04	0,43	0,00	0,02	0,03	0,02	0,00
	V11	0,04	0,00	0,02	0,01	0,00	0,00	0,01	0,14	0,04	0,02		0,29	0,01	0,00	0,00	0,01	0,00	0,00	0,00	0,00
	V12	0,00	0,01	0,24	0,06	0,00	0,01	0,17	0,27	0,19	0,26	0,29		0,08	0,01	0,02	0,08	0,00	0,01	0,11	0,00
	V13	0,00	0,09	0,00	0,00	0,00	0,01	0,02	0,46	0,00	0,13	0,01	0,08		0,00	0,00	0,05	0,02	0,04	0,00	0,00
	V14	0,00	0,00	0,09	0,00	0,01	0,00	0,00	0,02	0,02	0,04	0,00	0,01	0,00		0,00	0,00	0,00	0,00	0,00	0,00
	V15	0,00	0,00	0,01	0,00	0,01	0,02	0,04	0,41	0,30	0,43	0,00	0,02	0,00	0,00		0,01	0,00	0,00	0,00	0,00
	V16	0,01	0,05	0,00	0,01	0,00	0,00	0,00	0,00	0,01	0,00	0,01	0,08	0,05	0,00	0,01		0,00	0,00	0,02	0,01
	V17	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,02	0,00	0,00	0,02	0,00	0,00	0,00		0,00	0,00	0,00
	V18	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,03	0,00	0,01	0,04	0,00	0,00	0,00	0,00		0,00	0,00
	V19	0,01	0,01	0,01	0,00	0,00	0,00	0,01	0,08	0,00	0,02	0,00	0,11	0,00	0,00	0,00	0,02	0,00	0,00		0,00
	V20	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	

Fonte: Resultados da pesquisa (2009)

Tabela 108 – Matriz anti-imagem

		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20
Anti-image Covariance	V1	0,36	0,02	0,06	-0,16	0,03	0,07	-0,11	-0,04	-0,02	0,14	-0,03	-0,14	-0,06	0,01	0,06	-0,01	-0,04	-0,04	0,02	-0,14
	V2	0,02	0,58	0,00	0,10	0,00	0,05	-0,10	-0,04	-0,18	-0,06	-0,05	-0,12	0,04	-0,08	-0,13	0,08	-0,01	-0,05	-0,01	0,02
	V3	0,06	0,00	0,52	-0,06	-0,06	-0,01	-0,08	-0,04	-0,04	0,08	0,00	0,07	-0,10	0,12	-0,01	-0,10	-0,09	-0,01	0,02	-0,08
	V4	-0,16	0,10	-0,06	0,39	-0,04	-0,10	0,01	-0,01	-0,04	-0,10	0,05	0,08	-0,04	-0,07	-0,11	0,04	0,02	0,00	0,04	0,03
	V5	0,03	0,00	-0,06	-0,04	0,47	-0,05	-0,09	-0,10	0,05	0,05	-0,17	-0,19	-0,07	0,10	0,03	-0,03	0,00	-0,01	-0,07	-0,03
	V6	0,07	0,05	-0,01	-0,10	-0,05	0,40	0,00	-0,08	-0,11	-0,01	-0,07	-0,08	0,04	-0,06	0,07	0,06	-0,07	-0,09	-0,02	-0,04
	V7	-0,11	-0,10	-0,08	0,01	-0,09	0,00	0,50	-0,04	0,11	-0,17	0,02	0,10	0,01	-0,06	0,03	-0,07	0,03	0,00	-0,02	-0,02
	V8	-0,04	-0,04	-0,04	-0,01	-0,10	-0,08	-0,04	0,58	-0,08	-0,04	0,08	0,09	0,13	-0,06	0,05	-0,06	0,01	-0,02	-0,01	0,00
	V9	-0,02	-0,18	-0,04	-0,04	0,05	-0,11	0,11	-0,08	0,52	-0,10	-0,01	0,03	-0,13	0,06	0,07	-0,07	0,03	0,04	-0,02	-0,04
	V10	0,14	-0,06	0,08	-0,10	0,05	-0,01	-0,17	-0,04	-0,10	0,50	-0,08	-0,05	0,01	0,03	0,12	-0,08	-0,03	0,04	-0,06	-0,11
	V11	-0,03	-0,05	0,00	0,05	-0,17	-0,07	0,02	0,08	-0,01	-0,08	0,56	0,15	0,03	-0,10	-0,15	-0,02	0,01	0,03	-0,02	0,04
	V12	-0,14	-0,12	0,07	0,08	-0,19	-0,08	0,10	0,09	0,03	-0,05	0,15	0,59	0,02	-0,05	-0,03	-0,01	-0,07	0,04	0,03	0,00
	V13	-0,06	0,04	-0,10	-0,04	-0,07	0,04	0,01	0,13	-0,13	0,01	0,03	0,02	0,42	-0,16	0,01	0,03	0,00	0,07	-0,20	0,01
	V14	0,01	-0,08	0,12	-0,07	0,10	-0,06	-0,06	-0,06	0,06	0,03	-0,10	-0,05	-0,16	0,40	-0,06	-0,10	0,04	-0,04	0,00	-0,03
	V15	0,06	-0,13	-0,01	-0,11	0,03	0,07	0,03	0,05	0,07	0,12	-0,15	-0,03	0,01	-0,06	0,40	-0,03	-0,08	-0,02	-0,05	-0,12
	V16	-0,01	0,08	-0,10	0,04	-0,03	0,06	-0,07	-0,06	-0,07	-0,08	-0,02	-0,01	0,03	-0,10	-0,03	0,57	-0,14	-0,02	0,02	0,08
	V17	-0,04	-0,01	-0,09	0,02	0,00	-0,07	0,03	0,01	0,03	-0,03	0,01	-0,07	0,00	0,04	-0,08	-0,14	0,37	-0,13	0,01	-0,01
	V18	-0,04	-0,05	-0,01	0,00	-0,01	-0,09	0,00	-0,02	0,04	0,04	0,03	0,04	0,07	-0,04	-0,02	-0,02	-0,13	0,40	-0,12	-0,06
	V19	0,02	-0,01	0,02	0,04	-0,07	-0,02	-0,02	-0,01	-0,02	-0,06	-0,02	0,03	-0,20	0,00	-0,05	0,02	0,01	-0,12	0,56	0,03
	V20	-0,14	0,02	-0,08	0,03	-0,03	-0,04	-0,02	0,00	-0,04	-0,11	0,04	0,00	0,01	-0,03	-0,12	0,08	-0,01	-0,06	0,03	0,38
Anti-image Correlation	V1	0,77	0,04	0,15	-0,42	0,08	0,18	-0,25	-0,09	-0,05	0,34	-0,08	-0,30	-0,16	0,02	0,16	-0,03	-0,10	-0,09	0,03	-0,39
	V2	0,04	0,78	0,01	0,21	0,00	0,10	-0,19	-0,07	-0,32	-0,11	-0,08	-0,20	0,09	-0,16	-0,26	0,15	-0,02	-0,11	-0,02	0,05
	V3	0,15	0,01	0,85	-0,12	-0,13	-0,03	-0,16	-0,07	-0,09	0,15	0,00	0,12	-0,21	0,26	-0,03	-0,18	-0,21	-0,02	0,03	-0,19
	V4	-0,42	0,21	-0,12	0,84	-0,09	-0,25	0,03	-0,02	-0,09	-0,23	0,10	0,16	-0,09	-0,18	-0,29	0,09	0,05	-0,01	0,09	0,09
	V5	0,08	0,00	-0,13	-0,09	0,84	-0,11	-0,18	-0,20	0,09	0,09	-0,33	-0,36	-0,16	0,23	0,06	-0,06	0,00	-0,01	-0,13	-0,07
	V6	0,18	0,10	-0,03	-0,25	-0,11	0,88	0,01	-0,17	-0,24	-0,03	-0,15	-0,16	0,09	-0,16	0,19	0,13	-0,18	-0,22	-0,04	-0,09
	V7	-0,25	-0,19	-0,16	0,03	-0,18	0,01	0,84	-0,07	0,22	-0,35	0,03	0,18	0,03	-0,13	0,07	-0,14	0,06	0,01	-0,03	-0,05
	V8	-0,09	-0,07	-0,07	-0,02	-0,20	-0,17	-0,07	0,85	-0,15	-0,08	0,14	0,16	0,26	-0,13	0,11	-0,11	0,02	-0,05	-0,02	0,00
	V9	-0,05	-0,32	-0,09	-0,09	0,09	-0,24	0,22	-0,15	0,79	-0,19	-0,03	0,06	-0,28	0,13	0,15	-0,14	0,07	0,08	-0,04	-0,09
	V10	0,34	-0,11	0,15	-0,23	0,09	-0,03	-0,35	-0,08	-0,19	0,70	-0,16	-0,09	0,03	0,07	0,28	-0,15	-0,08	0,08	-0,11	-0,26
	V11	-0,08	-0,08	0,00	0,10	-0,33	-0,15	0,03	0,14	-0,03	-0,16	0,80	0,26	0,07	-0,21	-0,32	-0,04	0,03	0,05	-0,04	0,10
	V12	-0,30	-0,20	0,12	0,16	-0,36	-0,16	0,18	0,16	0,06	-0,09	0,26	0,67	0,03	-0,10	-0,07	-0,02	-0,15	0,08	0,05	0,00
	V13	-0,16	0,09	-0,21	-0,09	-0,16	0,09	0,03	0,26	-0,28	0,03	0,07	0,03	0,75	-0,38	0,03	0,06	-0,01	0,18	-0,41	0,02
	V14	0,02	-0,16	0,26	-0,18	0,23	-0,16	-0,13	-0,13	0,13	0,07	-0,21	-0,10	-0,38	0,83	-0,15	-0,20	0,10	-0,10	0,01	-0,09
	V15	0,16	-0,26	-0,03	-0,29	0,06	0,19	0,07	0,11	0,15	0,28	-0,32	-0,07	0,03	-0,15	0,78	-0,07	-0,20	-0,05	-0,11	-0,30
	V16	-0,03	0,15	-0,18	0,09	-0,06	0,13	-0,14	-0,11	-0,14	-0,15	-0,04	-0,02	0,06	-0,20	-0,07	0,85	-0,30	-0,03	0,04	0,18
	V17	-	-	-	0,05	0,00	-0,18	0,06	0,02	0,07	-0,08	0,03	-0,15	-0,01	0,10	-0,20	-0,30	0,89	-0,33	0,03	-

	0,10	0,02	0,21																	0,02
V18	-0,09	-0,11	-0,02	-0,01	-0,01	-0,22	0,01	-0,05	0,08	0,08	0,05	0,08	0,18	-0,10	-0,05	-0,03	-0,33	0,90	-0,25	-0,14
V19	0,03	-0,02	0,03	0,09	-0,13	-0,04	-0,03	-0,02	-0,04	-0,11	-0,04	0,05	-0,41	0,01	-0,11	0,04	0,03	-0,25	0,87	0,07
V20	-0,39	0,05	-0,19	0,09	-0,07	-0,09	-0,05	0,00	-0,09	-0,26	0,10	0,00	0,02	-0,09	-0,30	0,18	-0,02	-0,14	0,07	0,88

Fonte: Resultados da pesquisa (2009)

Tabela 109 – *Comunalidades*

Assertiva	Initial	Extraction
V1	1	0,7261321
V2	1	0,7133819
V3	1	0,6535932
V4	1	0,6568396
V5	1	0,4577583
V6	1	0,5919657
V7	1	0,4616237
V8	1	0,5977663
V9	1	0,6185052
V10	1	0,6656036
V11	1	0,6261479
V12	1	0,6380813
V13	1	0,7913848
V14	1	0,611495
V15	1	0,7461711
V16	1	0,5283014
V17	1	0,7137605
V18	1	0,6266052
V19	1	0,542057
V20	1	0,636607

Fonte: Resultados da pesquisa (2009)

Tabela 110 - Total de variância explicada

Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	7,258	36,291	36,291	7,258	36,291	36,291
2	1,711	8,553	44,843	1,711	8,553	44,843
3	1,34	6,701	51,544	1,34	6,701	51,544
4	1,217	6,083	57,627	1,217	6,083	57,627
5	1,078	5,392	63,019	1,078	5,392	63,019
6	0,966	4,83	67,848			
7	0,851	4,253	72,102			
8	0,779	3,895	75,997			
9	0,719	3,596	79,592			
10	0,689	3,445	83,038			
11	0,616	3,082	86,12			
12	0,452	2,26	88,38			
13	0,426	2,128	90,508			
14	0,385	1,924	92,432			
15	0,316	1,579	94,012			
16	0,306	1,532	95,543			
17	0,282	1,41	96,954			
18	0,245	1,223	98,176			
19	0,206	1,031	99,208			
20	0,158	0,792	100			

Fonte: Resultados da pesquisa (2009)

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo