Kelson Côrte

Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos

Brasília, DF

2014

Kelson Côrte

SEGURANÇA DA INFORMAÇÃO BASEADA NO VALOR DA INFORMAÇÃO E NOS PILARES TECNOLOGIA, PESSOAS E PROCESSOS

Tese apresentada à Faculdade de Ciência da Informação da Universidade de Brasília como requisito para a obtenção do título de Doutor em Ciência da Informação.

Orientador:
Professor Dr. Rogério Henrique de Araújo Júnior

Brasília, DF
2014

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 1016055.

Côrte, Kelson.
C827s Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos / Kelson Côrte. - - 2014.
212 f. : il. ; 30 cm.

Tese (doutorado) – Universidade de Brasília, Faculdade de Ciência da Informação, Programa de Pós-Graduação em Ciência da Informação, 2014.
Inclui bibliografia.
Orientação: Rogério Henrique de Araújo Júnior.

1. Ciência da informação. 2. Sistemas de recuperação da informação – Segurança. 3. Serviços de informação. I. Araújo Júnior, Rogério Henrique de. II. Título.

CDU 002:004

FOLHA DE APROVAÇÃO

Título: *"Segurança da Informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos".*

Autor (a): Kelson Côrte

Área de concentração: Transferência da Informação

Linha de pesquisa: Gestão da Informação

Tese submetida à Comissão Examinadora designada pelo Colegiado do Programa de Pós-graduação em Ciência da Informação da Faculdade em Ciência da Informação da Universidade de Brasília como requisito parcial para obtenção do título de **Doutor** em Ciência da Informação.

Tese aprovada em: 06 de junho de 2014

Prof. Dr. Rogério Henrique de Araújo Júnior
Presidente (UnB/PPGCINF)

Prof. Dr. Renato Tarciso Barbosa de Sousa
Membro Interno (UnB/PPGCINF)

Prof. Dr. Jorge Henrique Cabral Fernandes
Membro Interno (UnB/PPGCINF)

Prof. Dr. Carlos Blaya Perez
Membro Externo (UFSM)

Prof. Dr. Eduardo Amadeu Dutra Moresi
Membro Externo (UCB)

Profª. Drª. Dulce Maria Baptista
Suplente (UnB/PPGCINF)

À memória de meu pai, Abel Pereira Côrte,

que, com sua sabedoria, me fazia sentir seguro.

Agradecimentos

A Deus, por me sustentar em todas as dificuldades da vida;

À minha esposa, Dione Angélica, companheira em todas as circunstâncias e grande incentivadora;

À minha mãe, Maria Côrte, mulher de fé, amorosa e temente a Deus;

Aos meus filhos e às minhas filhas, que me inspiram com suas características individuais:

Fabio, pela alegria e pela energia inesgotável,

Gustavo, pela serenidade e pela profundidade intelectual,

Ana Clara, pela alegria de viver e pela persistência,

Luciana, pela autenticidade e pela determinação;

Ao meu orientador, Prof. Dr. Rogério Henrique de Araújo Júnior, pelo incentivo, por ter me feito enxergar além, por acreditar na minha capacidade e pela competente orientação;

Aos amigos mais próximos, que não me deixaram desistir.

Escutem! A Sabedoria está gritando nas ruas e nas praças. Nos portões das cidades e em todos os lugares onde o povo se reúne, ela está gritando alto, assim: "Até quando vocês, inexperientes, irão contentar-se com a sua inexperiência? Vocês, zombadores, até quando terão prazer na zombaria? E vocês, tolos, até quando desprezarão o conhecimento?"

Os tolos morrem porque rejeitam a sabedoria; os que não têm juízo são destruídos por estarem satisfeitos consigo mesmos. Mas quem ouvir a Sabedoria terá segurança, viverá tranquilo e não terá motivo para ter medo de nada (Provérbios 1:20-22, 32-33, NTHL).

Resumo

A informação tem se tornado algo cada vez mais importante para as organizações. Da mesma maneira que um ativo valioso demanda proteção, a informação deve ser protegida, principalmente contra as ameaças que afetam a sua integridade, a sua disponibilidade e a sua confidencialidade. Mesmo quando há preocupação com a segurança, em geral, os resultados obtidos não têm sido satisfatórios, acarretando prejuízos para organizações públicas e privadas, para cidadãos e, até mesmo, para nações. Assim, este estudo propõe um método de avaliação da segurança da informação baseado no valor da informação e nos pilares tecnologia, pessoas e processos. É proposta também, uma metodologia para a mensuração de cada um dos pilares, de tal forma que o possível desbalanceamento existente entre eles seja evidenciado. A pesquisa está dividida em três etapas: I. Revisão de literatura sobre os aspectos que envolvem a segurança da informação, com vistas a situá-los no âmbito da ciência da informação e estabelecer a fundamentação teórica; II. Apresentação das proposições do autor; e, III. Compilação e análise dos resultados da aplicação da metodologia proposta, realizada com os bancos estaduais: Banrisul, Banestes, BRB, Banese e Banpará. Durante a pesquisa, pôde-se verificar de que maneira os gestores estimam o valor da informação e, se utilizam esse valor como subsídio para definirem os requisitos de sua proteção. Verificou-se, também, o equilíbrio entre os pilares que sustentam a segurança da informação em cada instituição pesquisada. Concluiu-se que o valor da informação contribui significativamente para a definição dos requisitos de segurança da informação e, que a informação tende a estar mais bem protegida quando os pilares tecnologia, pessoas e processos estão em equilíbrio.

Palavras-chave: Ciência da informação. Segurança da informação. Valor da informação. Pilares tecnologia, pessoas e processos.

Abstract

The information has become something increasingly important for organizations. Like a valuable asset demand protection, the information must be protected, particularly against the threats to its integrity, availability and confidentiality. Even when there is concern about security, in general, the results have not been satisfactory, causing damage to public and private organizations, to citizens and even nations. Thus, this study proposes a method of assessment of information security based on the information value and on the pillars technology, people and processes. It also proposed a methodology for the measurement of each pillar, such that the possible imbalance existing between them can be demonstrated. The research is divided into three steps: I. Review of literature on aspects that involve the information security, in order to situate them in the context of information science and to establish the theoretical ground II. Presentation the author propositions, and III. Compilation and analysis of survey results with state banks: Banrisul Banestes, BRB, Banese and Banpará. During the research, it could be checked how the managers estimate the value of information and if they use this value as an input to define the requirements to protect it. It also could be checked the balance between the pillars that support the information security at each research institution. It was concluded that the value of information contributes significantly to defining the information security requirements and that the information tends to be better protected when the pillars technology, people and processes are in equilibrium.

Keywords: Information science. Information security. Value of information. Pillars technology, people and processes.

Relação das figuras

Relação dos quadros

Relação dos gráficos

Relação das tabelas

Lista de siglas

ABNT - Associação Brasileira de Normas Técnicas

APF - Administração Pública Federal

ARPANET - *Advanced Research Projects Agency Network*

BACEN - Banco Central do Brasil

BANESE - Banco do Estado do Sergipe

BANESTES - Banco do Estado do Espírito Santo

BANPARA - Banco do Estado do Pará

BANRISUL - Banco do Estado do Rio Grande do Sul

BDTD - Biblioteca Digital Brasileira de Teses e Dissertações

BERR - *Department for Business Enterprise & Regulatory Reform*

BRAPCI - Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação

BRB - Banco de Brasília S/A

BSC - *Balanced Scorecard*

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CERT - *Computer Emergence Response Team*

CI - Ciência da Informação

CIA - *Central Intelligence Agency*

CIO - *Chief Information Office*

COBIT - *Control Objectives for Information and Related Technology*

CSI - *Computer Security Institute*

CSO - *Chief Security Office*

DMAIC – Definir, Medir, Analisar, Implentar e Controlar

DoD - *Department of Defense*

DSIC - Departamento de Segurança da Informação e Comunicação

ECT - Empresa Brasileira de Correios e Telégrafos

FBI - *Federal Bureau of Investigation*

FEBRABAN - Federação Brasileira de Bancos

GI - Gestão da Informação

GSI/PR - Gabinete de Segurança Institucional da Presidência da República

HUSM - Hospital Universitário de Santa Maria

IBGE - Instituto Brasileiro de Geografia e Estatística

IBICT - Instituto Brasileiro de Informação em Ciência e Tecnologia

ISO - *International Organization for Standardization*

ISTA - *Information Science & Technology Abstracts*

ITIL - *Information Technology Infrastructure Library*

LAN – *Local Area Network*

LISA - *Library and Information Science Abstracts*

LISTA - *Library, Information Science & Technology Abstracts*

NIST - *National Institute of Standards and Technology*

OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation*

PQDT - *ProQuest Dissertation & Theses*

PSI - Política de Segurança da Informação

RS - Rio Grande do Sul

SCADA - *Supervisory, Control and Data Acquisition*

SEI - *Software Engineering Institute*

SGSI - Sistema de Gestão de Segurança da Informação

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

TRI - Teoria da Resposta ao Item

UCI - Unidades de Cardiologia Intensiva

USA - *United States of America*

UTI - Unidade de Terapia Intensiva

VDI - Valor da Informação

Sumário

1 Introdução

A informação sempre foi um ativo importante para todos os segmentos da sociedade. Porém, até meados do século passado, havia grande dificuldade em acessar, em capturar, em tratar e em disseminar informações. Naquele contexto, o risco de se tomar uma decisão errada era muito alto, uma vez que as informações que deveriam dar suporte às decisões eram escassas, de precisão duvidosa e ainda de baixa disponibilidade. Hoje, em grande parte devido à evolução tecnológica, a geração, o acesso e a disseminação de informações têm sido algo muito mais simples e mais rápido. Como consequência, o volume de informações disponíveis tem alcançado patamares tão elevados que um dos grandes problemas deste século, ao contrário dos séculos passados, deverá ser a superabundância de informações.

Ter a informação certa, na hora certa, pode dar o direcionamento certo às organizações. McGee e Prusak (1994) afirmam que a informação é fator fundamental para a definição de estratégia. Para Choo (2003), as organizações utilizam a informação para dar sentido às mudanças do ambiente externo e, principalmente, como fator de suporte às decisões.

O intervalo de tempo entre a inovação e a aplicação comercial dela tem reduzido de forma célere e o ciclo de vida dos produtos está cada vez menor. O mercado lança novos produtos e novos serviços a cada dia, e o que é novo se torna obsoleto rapidamente. Da mesma forma, tem ocorrido com a geração e a disponibilização de informações. No entanto, apesar desse volume imenso de informações, ao contrário do que se esperava, tem-se verificado uma incômoda sensação de insegurança, como se alguma informação já disponível no mercado não tivesse sido considerada, no momento da tomada de decisão. Essa sensação é compatível com o que Beck (1992) denominou de "sociedade de risco", cujo conceito se cruza diretamente com o de globalização: os riscos são democráticos, porque afetam nações e classes sociais, sem respeitar nenhum tipo de fronteira. Entre esses riscos, inclui os riscos ecológicos, químicos, nucleares e genéticos, produzidos

industrialmente, externalizados economicamente, individualizados juridicamente, legitimados cientificamente e minimizados politicamente. Mais recentemente, o autor incorporou também aos seus conceitos os riscos econômicos, como as quedas nos mercados financeiros internacionais. Esse conjunto de riscos geraria "uma nova forma de capitalismo, uma nova forma de economia, uma nova forma de ordem global, uma nova forma de sociedade e uma nova forma de vida pessoal" (BECK, 1992).

No campo da informação, as organizações estão enfrentando o grande desafio da carência de capital humano competente para identificar, em um mar de informações, aquelas que lhes são úteis e lhes tragam vantagens competitivas, e que estão espalhadas em meio a uma sociedade de alto risco.

Nesse contexto, a informação certa tem adquirido valor estratégico tão elevado a ponto de se tornar o principal ativo de uma organização, cujo uso pode determinar o seu grau de sucesso ou de fracasso. Sêmola (2003) afirma que a informação representa a inteligência competitiva dos negócios, a qual é reconhecida como ativo crítico para a continuidade operacional e a saúde da empresa. Em um ponto de vista complementar, Rezende e Abreu (2003) defendem que a informação possui um valor altamente significativo e que pode representar grande poder para quem a detém.

Observando a crescente importância estratégica da informação Drucker (1993) previu a troca do binômio capital/trabalho pelo binômio informação/conhecimento, como fator determinante do sucesso empresarial. Assim, o mundo pode estar caminhando para a sociedade do saber ou do conhecimento, em que a informação deverá suplantar, em importância, o capital para que as organizações formulem suas estratégias, promovam seus negócios e cumpram sua missão.

Por ser um ativo de alto valor estratégico, a informação precisa ser tratada com cuidados especiais e ser protegida adequadamente. Esses aspectos são abordados na Norma NBR ISO/IEC 27.002:2005 que define segurança da informação

"como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ASSOCIAÇÃO, 2005).

Esta pesquisa abordou o valor da informação e o balanceamento entre os pilares tecnologia, pessoas e processos, visando subsidiar ações de segurança da informação. Além das etapas de apresentação do problema a ser investigado, justificativa, objetivos geral e específicos, dedicou-se um capítulo à revisão de literatura, no qual se situou o problema dentro da área de estudo, que é a ciência da informação e estabeleceu-se a fundamentação teórica. Foram apresentadas as proposições do autor e, por fim, fez-se uma análise dos resultados da pesquisa de campo realizada com os bancos estaduais, Banco do Estado do Rio Grande do Sul - Banrisul, Banco do Estado do Espírito Santo - Banestes, Banco de Brasília - BRB, Banco do Estado do Sergipe - Banese e Banco do Estado do Pará - Banpara, visando verificar os pressupostos e formular as teses.

1.1 Tema e problema

1.1.1 Tema

Avaliação da segurança da informação a partir da estimativa do valor da informação e do balanceamento entre os pilares tecnologia, pessoas e processos.

1.1.2 Problema

Uma instituição bancária lida diariamente com um grande volume de informações geradas por ela mesma e por outras organizações, como resultado da relação com seus clientes e seus fornecedores. Assim sendo, um banco, como parte ativa de um ecossistema complexo, precisa estar constantemente atualizado acerca das inúmeras informações produzidas pelo mercado financeiro mundial, como, por exemplo, indicadores dos mais variados componentes da economia. Não basta estar atento apenas às informações locais, pois a economia funciona como uma grande e complexa engrenagem e, assim, as mudanças na economia ou na política de um país

podem ter repercussões imediatas em muitos outros países. Além disso, os órgãos reguladores e fiscalizadores também são grandes geradores de informações na atividade bancária. Esses órgãos impõem aos bancos a obrigatoriedade de estar em conformidade com o arcabouço normativo.

As decisões tomadas pelo setor financeiro são muito sensíveis, as quais refletem diretamente em vários outros setores e, principalmente, sobre o consumidor. Toda decisão provoca uma consequência correspondente, seja positiva, seja negativa. Por isso, convém que toda decisão esteja fundamentada em informações seguras e consistentes. Uma simples declaração de uma autoridade monetária é capaz de alterar o comportamento das ações na bolsa de valores, provocar a remarcação dos preços das mercadorias nos supermercados e, até mesmo, é capaz de influenciar o preço de mercadorias no mercado internacional.

Por lidar com assuntos tão sensíveis, o setor financeiro é um dos mais regulamentados do país. Leis como a do sigilo bancário impõem a obrigatoriedade não somente de preservar, mas também de proteger as informações da clientela, sob pena de sanções severas a quem descumpri-las. Um caso amplamente divulgado pela imprensa foi o do ex-Ministro da Fazenda Antonio Palocci Filho, afastado de suas funções por ter ordenado, em março de 2006, ao então presidente da Caixa Econômica Federal, Jorge Mattoso, que violasse o sigilo bancário do caseiro Francenildo Costa (OLTRAMARI, 2008).

Outras regulamentações como os acordos de Basileia[1] I, II e III, Sarbanes-Oxley[2] e a Resolução nº 3.380, do Banco Central do Brasil (BANCO, 2006), impuseram também às instituições financeiras a obrigatoriedade de desenvolverem ações para gerirem os riscos operacionais, além da gestão cuidadosa de riscos de

[1] Acordo proposto pelo Comitê de Supervisão Bancária, com sede na cidade de Basiléia (Suíça), visando o fortalecimento da solidez dos sistemas financeiros, através do controle de riscos, transparência e governança corporativa (DERMEVAL, 2014).

[2] Lei promulgada nos Estados Unidos em julho de 2002, com foco na transparência dos registros contábeis (THE SARBANES-OXLEY ACT, 2013).

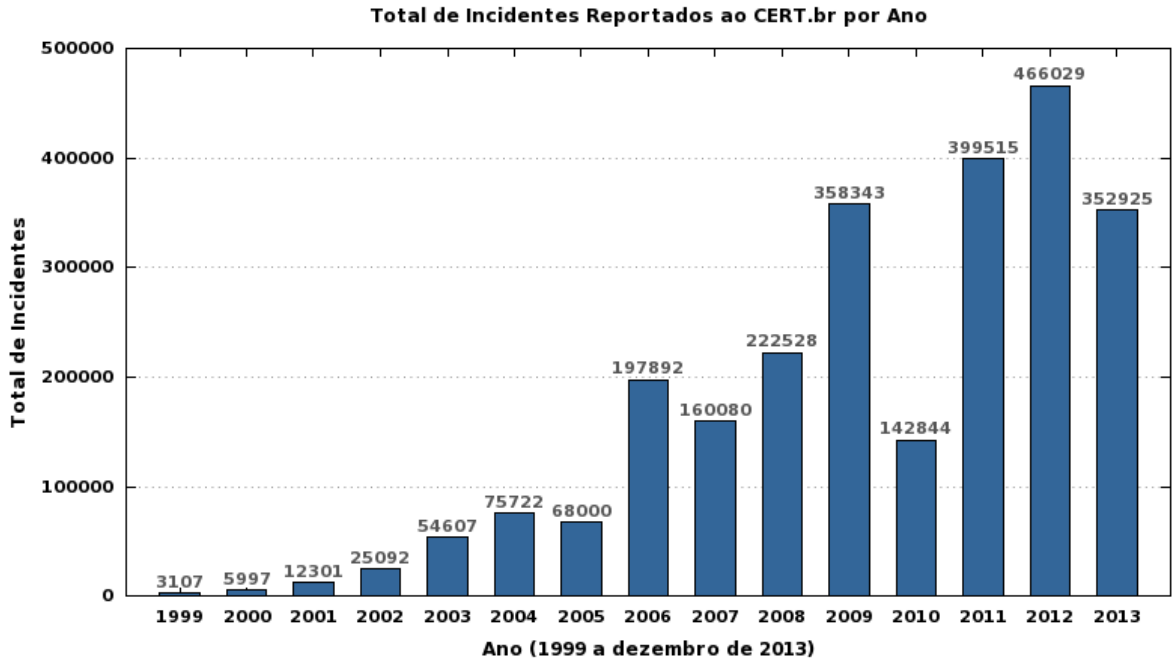
crédito, de liquidez e de mercado, a que já estavam anteriormente obrigadas. O sigilo, a proteção e a segurança da informação são aspectos tratados pelo risco operacional. O banco que não atender ou atender parcialmente os critérios normativos do risco operacional deverá reservar um volume de dinheiro, calculado com metodologia específica, com o qual não poderá operar. Essa reserva destina-se a cobrir possíveis perdas operacionais, como por exemplo, incidentes de segurança da informação, tais como: fraudes, clonagens de cartões, roubos de senhas, entre outros.

Segundo a Febraban, a quantia perdida por fraude e o gasto necessário para combatê-la representam efetivamente um custo para a sociedade. Os efeitos disso são sentidos diretamente pelas instituições atingidas e, indiretamente, pelos consumidores, com a alta das tarifas, ou com procedimentos mais rígidos para a abertura de contas e, também, para atribuir escrutínio das suas transações (FEDERAÇÃO, 2004).

Ocorre que muitas instituições, financeiras ou não, públicas ou privadas, mesmo sabendo da importância estratégica de preservar suas informações, têm dificuldades na gestão da segurança.

A *Carnegie Mellon University* – USA mantém o CERT **-** *Computer Emergency Response Team*, que é parte do *Software Engineering Institute* - SEI. O seu braço no Brasil (CERT.br) é o Grupo de Resposta a Incidentes de Segurança para a Internet Brasileira, mantido pelo Comitê Gestor da Internet no Brasil. A Estatística dos Incidentes Reportados ao CERT.br, conforme gráfico 1, evidencia o crescente número de incidentes ocorridos e relatados no Brasil. É provável que esse número seja superior ao apresentado no gráfico 1, uma vez que nem todos os incidentes são devidamente reportados ao CERT.

Gráfico 1 - Total de Incidentes Reportados ao CERT.br por ano.



Fonte: Cert.br. Estatísticas dos Incidentes Reportados ao CERT.br.
Disponível em: www.cert.br/stats/incidentes/. Acesso em: 20 mar. 2014.

Contribui para essa estatística, a pesquisa encomendada em 2008 pelo BERR - *Department for Business Enterprise & Regulatory Reform* (REINO UNIDO, 2008), conduzida pela *PriceWaterhouseCoopers*[3], a qual constatou que 96% das grandes empresas tiveram algum incidente de segurança em 2007.

Em junho de 2011, ocorreram vários incidentes no Brasil, quando *hackers* invadiram *sites* de órgãos oficiais, tais como: Presidência da República, Portal Brasil, Receita Federal e IBGE (SALATIEL, 2011). Esses *sites* ficaram fora do ar por algumas horas, prejudicando os serviços prestados. Segundo as autoridades competentes, os dados armazenados nesses *sites* não foram alterados nem roubados. Porém, a falha foi exposta e as consequências poderiam ter sido grandes. Por exemplo, muitas políticas sociais do governo são elaboradas com base em pesquisas do IBGE e, caso esses dados sejam alterados, tais políticas poderão estar completamente equivocadas e, dessa forma, gerarem prejuízos para toda a nação. Naquele mesmo mês, um *hacker* divulgou supostos dados pessoais de diversos

[3] Empresa multinacional especializada em consultoria e auditoria.

políticos. Tais dados teriam sido obtidos mediante a invasão a *sites* de órgãos públicos, que não souberam proteger as informações sob sua guarda.

A mídia também divulgou a invasão aos *sites* da Sony no Canadá, na Grécia, na Tailândia, dos quais foram roubados dados de cem milhões de contas de usuários, incluindo-se *e-mails*, senhas e cartões de crédito (RIBEIRO, 2013). Muitos outros *sites* famosos foram invadidos recentemente, como ocorreu com o FBI, a CIA, a rede de televisão americana Fox e o videogame Nintendo (SALATIEL, 2011).

Outra questão que tem preocupado as autoridades é a guerra cibernética que, segundo Parks e Duggan (2001), é o subconjunto da guerra da informação que envolve ações realizadas no mundo. Em março de 2012, um exercício militar internacional realizado em uma base militar na Estônia, tentou prever as consequências desse novo tipo de conflito. A operação conhecida como *Locked Shields* não envolveu explosões, nem tanques, nem armas, mas uma equipe de especialistas em TI, que atacou outras nove equipes, espalhadas por toda a Europa (BBC, 2012).

Segundo Clarke (2010), assistente de combate ao terrorismo e segurança cibernética dos presidentes americanos Bill Clinton e George W. Bush, ataques cibernéticos mais sofisticados podem descarrilar trens, causar blecautes, não apenas mediante o corte do fornecimento de energia, mas podem danificar geradores, de forma permanente, que levariam meses para serem substituídos. Tais ataques podem causar grandes danos como explosões em oleodutos ou em gasodutos, podem impedir que aeronaves decolem e podem, também, causar tantos outros danos graves. Nesse cenário, um país com pouco ou sem poder bélico pode afrontar uma grande nação com ameaças reais de provocar danos irreparáveis, caso consiga invadir os sistemas de segurança dessa nação.

Segurança da informação, portanto, deixou de ser uma questão apenas de interesse privado ou público, mas agora é, também, uma questão de segurança nacional, que as nações não podem mais desprezar.

Algumas matérias divulgadas na mídia sobre incidentes[4] de segurança da informação estão disponíveis no Anexo 2.

Mesmo reconhecendo a importância estratégica de suas informações e as possíveis consequências advindas de falhas no processo de segurança, as empresas não estão conseguindo proteger adequadamente suas informações, o que as leva a contabilizar prejuízos significativos. Existe uma lacuna entre a intenção de proteger e o resultado efetivo das ações de proteção da informação. Com o objetivo de entender melhor esse problema, esta pesquisa dedicou-se a estudar a seguinte questão: **Como o valor da informação e os pilares tecnologia, pessoas e processos podem subsidiar ações de segurança da informação?**

2 Justificativa

Costuma-se proporcionar segurança a tudo aquilo que possui valor e, que, consequentemente, demanda proteção (RAMOS, 2008). Essa é uma afirmação abrangente que pode ser aplicada nas mais diferentes áreas da vida, tais como: material, sentimental, espiritual, cultural, científica. Quando o assunto é a informação, esse princípio também pode ser aplicado, porque **toda informação que possui valor deve ser protegida.**

Portanto, as organizações precisam se preocupar em proteger suas informações de valor. No entanto, muitas delas se dão conta dessa necessidade somente depois de serem acometidas por algum incidente que as tenha exposto a riscos e, não raramente, levado tais organizações a perdas elevadas. Outras, aparentemente, já compreenderam a importância de proteger suas informações e, em resposta, fizeram alguns investimentos, mas ainda estão longe de possuírem uma política de segurança consistente, compatível com o valor estratégico de seus ativos informacionais. A sobrevivência de uma organização pode estar ligada não somente às informações que ela detém, mas também na forma como essas

[4] Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade. (SUPERINTENDENCIA, 2014).

informações são manipuladas. A pior de todas as situações refere-se àquelas organizações que, por não terem a dimensão correta do risco a que estão sujeitas, têm a falsa sensação de segurança, o que faz com que deixem de tomar medidas para proteger adequadamente suas informações.

Talvez o maior exemplo deste século seja o ataque, em 11/09/2001, às torres gêmeas, em Nova Iorque, nos Estados Unidos, quando muitas organizações que tinham escritórios naqueles prédios perderam suas informações, apesar de terem feito altos investimentos em segurança, a ponto de possuírem dois *sites* para armazenar suas informações. O *site* principal ficava em uma torre e o de contingência em outra (CLUSTERS, 2009). Como a informação, segundo Sêmola (2003), representa a inteligência competitiva dos negócios, muitas empresas têm sido abaladas por não conseguirem proteger adequadamente as suas informações.

Segundo estimativas da consultoria americana *Ponemon Institute*, especializada em segurança da informação entre empresas, as perdas da *Sony Entertainment Television*, após seu *site* ter sido invadido por *hachers* em abril de 2011, devem girar entre US$ 1,5 bilhão e US$ 2 bilhões (FUSCO; PAIVA, 2011)

A Pesquisa Global em segurança da informação (PRICEWATERHOUSECOOPERS, 2013) revela quão impactantes são os incidentes de segurança no Brasil: (1) perdas financeiras (37%); (2) perdas de clientes (24%); (3) comprometimento da marca/reputação (21%). Além disso, segundo a pesquisa, cerca de 20% dos respondentes disseram que suas operações ficaram indisponíveis por até três horas, em decorrência de incidentes de segurança. No quesito financeiro, 31% dos respondentes no Brasil afirmam que as perdas decorrentes de incidentes de segurança foram inferiores a dez mil dólares e 4% mensuram as perdas em níveis acima de dez milhões de dólares. Ou seja, a sofisticação e a profissionalização dos "cibercriminosos" têm causado prejuízos relevantes para muitas organizações.

Os dados relacionados a incidentes em segurança da informação serão, na maioria das vezes, aproximado, uma vez que, segundo Gordon (2005),

43% das empresas que sofrem algum tipo de intrusão não declaram nem registram o incidente, principalmente devido à publicidade negativa que o ocorrido pode causar à imagem da empresa.

Algumas empresas precisam proteger suas informações por exigências do negócio, ou por força de lei, como a do sigilo bancário e fiscal[5], a do sigilo telefônico[6], por isso investem um pouco mais em segurança. Nesse rol, encontram-se, por exemplo, as instituições bancárias, a Receita Federal, as secretarias estaduais de fazenda e as empresas de telecomunicações.

Porém, apesar do investimento realizado e do esforço empreendido, os incidentes de segurança e as perdas financeiras decorrentes deles continuam crescentes, e fazem com que o resultado final das ações não seja o esperado. Tratar adequadamente essa questão é um desafio complexo e sensível que reflete diretamente na imagem e nos negócios das organizações.

Assim, é importante que se realizem pesquisas, visando entender melhor o problema, a fim de buscar alternativas para preencher a lacuna existente entre a intenção de proteger e o resultado efetivo das ações de proteção de informações. Com base nisso e com essa finalidade que este estudo se justificou.

3 Objetivos

3.1 Objetivo geral

Propor um método de avaliação da segurança da informação baseado no valor da informação e nos pilares tecnologia, pessoas e processos, de modo a subsidiar ações de proteção da informação em instituições bancárias.

3.2 Objetivos específicos

3.2.1 Verificar como os gestores, em instituições bancárias, estimam o valor da informação.

[5] Lei Complementar 105/2001
[6] Lei 9.296/96

3.2.2 Verificar se os gestores, em instituições bancárias, utilizam o valor da informação como subsídio para a definição dos requisitos de sua proteção.

3.2.3 Propor uma metodologia de medição dos pilares tecnologia, pessoas e processos, de tal maneira que o possível desequilíbrio existente entre eles possa ser evidenciado.

3.2.4 Estudar a aplicabilidade da avaliação do equilíbrio dos pilares tecnologia, pessoas e processos nas ações de segurança da informação.

4 Revisão de literatura

A produção do conhecimento não é um empreendimento isolado. É uma construção coletiva, um processo continuado de busca, no qual cada nova investigação se insere, complementando ou contestando contribuições anteriormente dadas ao estudo do tema. A proposição adequada de um problema de pesquisa exige, portanto, que o pesquisador se situe nesse processo, a fim de analisar criticamente o estado atual do conhecimento em sua área de interesse. Dessa forma, é possível ao pesquisador comparar e sobrepor abordagens teórico-metodológicas, bem como avaliar a confiabilidade de resultados de pesquisa, de modo a identificar pontos de consenso, assim como de controvérsias e também lacunas que merecem ser esclarecidas.

4.1 Contextualização do problema no âmbito da área de estudo

4.1.1 A ciência da informação e a segurança da informação

Segundo Silva e Freire (2012), não há um contributo principal para o advento da ciência da informação, mas um conjunto de ideias, de questões e de reflexões foram cruciais para a sua constituição como um campo do conhecimento científico. Isso ocorre devido à fragmentação dos componentes que influenciaram a origem da ciência da informação, uma vez que cada fator contribuiu para que a ciência da informação surgisse. O que é comum nesses fatores é a preocupação de preservar as informações geradas para uso futuro.

Le Coadic (1996) afirma que a informação é o sangue da ciência, e sem a qual a ciência não pode se desenvolver nem existir; a pesquisa seria inútil; e, o conhecimento não existiria. A ciência evolui a partir de resultados obtidos em experimentos anteriores e por isso o valor da informação científica é inestimável. O inglês Isaac Newton, pai da mecânica clássica, ao reconhecer a importância dos que o antecederam, afirmou que, se enxergou mais longe que outros homens, foi porque se ergueu sobre ombros de gigantes (BRENNAN, 2000). Essa afirmação mostra, de forma inequívoca, a necessidade de se guardar, de se proteger e de se preservar com integridade os resultados de pesquisas anteriores, para que a evolução da ciência ocorra sobre bases confiáveis.

Do ponto de vista epistemológico, a ciência da informação, que possui por objeto de estudo a informação, preocupa-se com a análise dos processos de construção, de comunicação e de uso da informação, bem como com a concepção dos produtos e dos sistemas que permitem sua organização, sua comunicação, seu armazenamento e seu uso (LE COADIC, 1996). Essa definição aponta a necessidade de um conhecimento multidisciplinar, que engloba, inclusive, a segurança da informação, uma vez que esta deve ser requerida em todos os pontos de preocupação da ciência da informação, descritos pelo autor. Além disso, o autor afirma que um dos objetivos da ciência da informação é investigar as propriedades e o comportamento da informação, bem como o acompanhamento e a análise do seu fluxo, visando oferecer o uso e o acesso adequados à informação requisitada. Nesse aspecto, o relacionamento entre a ciência da informação e a segurança da informação ocorre no esforço para se preservar a integridade da informação a ser usada e na garantia do acesso adequado, a fim de permitir que somente pessoas autorizadas possam acessar a informação requisitada e, que, para essas pessoas, a informação esteja disponível.

Borko (1968) define a ciência da informação como a disciplina que investiga as propriedades e o comportamento da informação, as forças que regem o fluxo informacional e os meios de processamento da informação para a otimização do acesso e do uso. Tal disciplina está relacionada com um corpo de conhecimento

que abrange a origem, a coleta, a organização, o armazenamento, a recuperação, a interpretação, a transmissão, a transformação e a utilização da informação. Esses aspectos dão suporte, para que a informação gerada ou capturada possa ser guardada e preservada com integridade, pelo período de tempo necessário, a fim de que possa ser recuperada e utilizada posteriormente. Porém, a informação está sob constante risco, em qualquer uma das etapas de seu ciclo de vida, razão pela qual deve ser protegida contra vários tipos de ameaças. O principal objetivo da segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação. Além disso, se preocupa com a identificação de vulnerabilidades e a gestão dos riscos associados aos diversos ativos informacionais, independentemente da forma ou do meio em que são compartilhados ou armazenados. Dessa forma, a segurança da informação deve contemplar todos os itens que compõem o corpo de conhecimento da informação, para que, ao ser utilizada no futuro, a informação seja a mesma gerada no passado, com suas propriedades e suas características preservadas.

A concepção de interdisciplinaridade da ciência da informação defendida, dentre outros, por Saracevic (1995), sustenta que os problemas que envolvem a informação não podem ser abordados dentro de uma única área da atividade científica. Bates (1999), corrobora essa concepção ao afirmar que a ciência da informação é uma metaciência que corta transversalmente várias disciplinas convencionais, e que tem como domínio o universo da informação registrada, selecionada e mantida para acesso futuro. A segurança da informação, também de forma multidisciplinar e cooperativa com a ciência da informação, propicia meios para manter a informação íntegra e garantir o acesso, no futuro, somente àqueles autorizados a fazer uso dela.

Fernandes (2010) também discute a possibilidade da inserção da segurança da informação no âmago da ciência da informação e, para tanto, baseou-se no mapa de conhecimento da ciência da informação proposto por Zins (2007). Esse mapa é o resultado de um estudo conduzido de 2003 a 2005, que foi publicado em uma série de quatro artigos no qual o autor utiliza a metodologia Delphi.

O estudo contemplou as respostas de 57 líderes acadêmicos em ciência da informação de 16 países, para as seguintes questões: 1) definições de conceitos fundamentais de dados, de informação, de conhecimento e de mensagem; 2) concepções alternativas em relação ao domínio da ciência da informação; 3) diferentes mapeamentos classificatórios da área; e 4) mapeamento compreensivo da ciência da informação. O autor propõe a organização da área em uma taxonomia com dez facetas, a saber: fundamentos multidisciplinares, fontes, trabalhadores do conhecimento, conteúdos, aplicações, operações e processos, tecnologias, ambientes, organizações e usuários.

Segundo Fernandes (2010), se a segurança da informação aderir à organização proposta por Zins, então é provável que ela seja um modelo para a ciência da informação. Após explorar cada um dos elementos, o autor acredita que os princípios, as práticas e os modelos da segurança da informação se mostram aderentes ao modelo de Zins e, além disso, sugere que a segurança da informação possa agregar algumas contribuições à ciência da informação, tais como, noções de identidade, individualidade, risco e reflexividade.

Como se pode observar a seguir, a informação é vista por vários autores como um ativo de valor, que pode ser útil para finalidades diversas:

- LESCA E ALMEIDA (1994):
    - A informação como fator de apoio à decisão;
    - A informação como fator de produção;
    - A informação como fator de sinergia;
    - A informação como fator determinante de comportamento.
- McGEE E PRUSAK (1994):
    - A informação como fator fundamental para a definição de estratégia;
    - A informação como ferramenta para a execução de estratégias;
    - A informação como fator de aprendizado organizacional.

- CHOO (2003):
    - A informação para dar sentido às mudanças do ambiente externo;
    - A informação como modo de gerar novos conhecimentos por meio do aprendizado;
    - A informação como fator de suporte às decisões.

Ao avaliar os pontos de vista desses autores, nota-se que a informação possui muitas e diferentes utilidades. O estudo das propriedades e do comportamento da informação, bem como o acompanhamento e a análise do seu fluxo, empreendidos pela ciência da informação, proporcionam as condições organizacionais e estruturantes necessárias para que a informação tenha a potencialidade de ser usada para várias e distintas finalidades. A segurança da informação contribui para desenvolver os meios, visando garantir, pelo menos, a confidencialidade, a integridade e a disponibilidade, igualmente necessárias para que a informação possa atingir adequadamente a finalidade pretendida.

Sobre a relação entre os objetos de estudo, segundo Le Coadic (1996), o objeto de estudo da ciência da informação é a informação. Já o objeto de estudo da segurança da informação ainda não está definitivamente estabelecido. No entanto, segundo Ramos (2008), costuma-se adotar medidas de segurança para proteger tudo aquilo que possui valor. Assim sendo, pressupõe-se que, se se quer proteger uma informação é porque ela tem valor. Dessa forma, o principal foco da segurança da informação é a informação que possui valor, uma vez que esta demanda proteção. Ocorre que toda informação que possui valor é, antes de tudo, informação e consequentemente de interesse da ciência da informação. Assim, utilizando-se a teoria dos conjuntos, tem-se que o objeto de estudo da ciência da informação contém o objeto de estudo da segurança da informação.

Mesmo que não haja consenso sobre os limites de abrangência da ciência da informação, poucos são os estudos sobre segurança da informação realizados dentro dessa ciência, como ficou evidenciado no capítulo 4 – Revisão de Literatura. Porém, ainda que não apareça de forma explícita, é possível perceber no

pensamento de diversos autores da área, a preocupação com a segurança da informação.

Bush (1945), por exemplo, entende que a informação deve ser sistematizada e preservada, para que possa ser utilizada em tempo futuro. Essa possibilidade de, posteriormente, tornar a informação acessível para usuários específicos, tornou-se um dos pontos fundamentais para a ciência da informação. Outra atividade dessa ciência é o estudo do fluxo da informação, isto é: onde se origina e por onde passa, até o seu descarte. O objetivo do estudo do fluxo é mapear esse percurso, sempre com vistas ao uso futuro da informação. Ou seja, recuperação confiável, com qualidade, cortada sob medida para o usuário. Para que isso seja possível, é recomendável que a informação esteja armazenada em ambiente seguro, com os requisitos apropriados de proteção contra as diversas ameaças, de forma que o seu acesso seja permitido somente a usuários autorizados.

Proteger a informação para recuperação e uso futuro é papel da segurança da informação. Nota-se, portanto, que há uma forte inter-relação entre ciência da informação e segurança da informação. Assim, seria apropriado que, nos domínios da ciência da informação, se abrissem mais espaços para o estudo aprofundado da segurança da informação.

Existem outras áreas que estudam a segurança da informação, porém cada uma delas se dedica mais detalhadamente aos aspectos próprios da sua área e não de forma abrangente, com a preocupação de agrupar os vários aspectos que envolvem a segurança. A ciência da computação, por exemplo, dedica-se mais aprofundadamente aos aspectos tecnológicos da segurança da informação; na administração se estudam, com muita propriedade, os aspectos relacionados aos processos. Já os aspectos relacionados a pessoas são estudados por várias áreas, como administração, psicologia, pedagogia, dentre outras. Porém, o estudo com visão multidisciplinar é próprio da ciência da informação, pois isso está em sua gênese. Assim sendo, parece ser apropriado que a segurança da informação seja objeto de interesse também da ciência da informação, a qual poderia estudá-la com

uma visão mais holística, de modo a reunir os diversos aspectos que a envolvem, bem como a inter-relação existente entre eles.

4.1.2 Trabalhos correlatos

Com o intuito de constatar a existência de trabalhos na literatura nacional e também na internacional sobre segurança da informação na ciência da informação, realizou-se uma extensa pesquisa nas bases de dados da Capes, notadamente nas bases *LISA - Library and Information Science Abstracts, LISTA - Library, Information Science & Technology Abstracts, ISTA - Information Science & Technology Abstracts (ISTA), ProQuest Dissertation & Theses (PQDT, A&I), ProQuest Science Journals (Articles)*, e na BRAPCI - Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação, bem como em outras bases, como as disponíveis no *Information Resource Center* da Biblioteca da Embaixada dos EUA em Brasília: *EBSCO, Library & Information Science, ProQuest Research Library (Science & Technology, Social Sciences, History, Literature & Language, Health & Medicine, Business, The Arts)* e na Biblioteca Digital Brasileira de Teses e Dissertações - BDTD do Instituto Brasileiro de Informação em Ciência e Tecnologia – IBICT.

Para tanto, nessa pesquisa, foram sobrepostos os termos "ciência da informação" e "segurança da informação", em português e em inglês, e poucos trabalhos foram encontrados. Um dele foi a tese de doutorado de Marciano (2006), defendida na Universidade de Brasília, sob o título: *Segurança da Informação: uma abordagem social.*

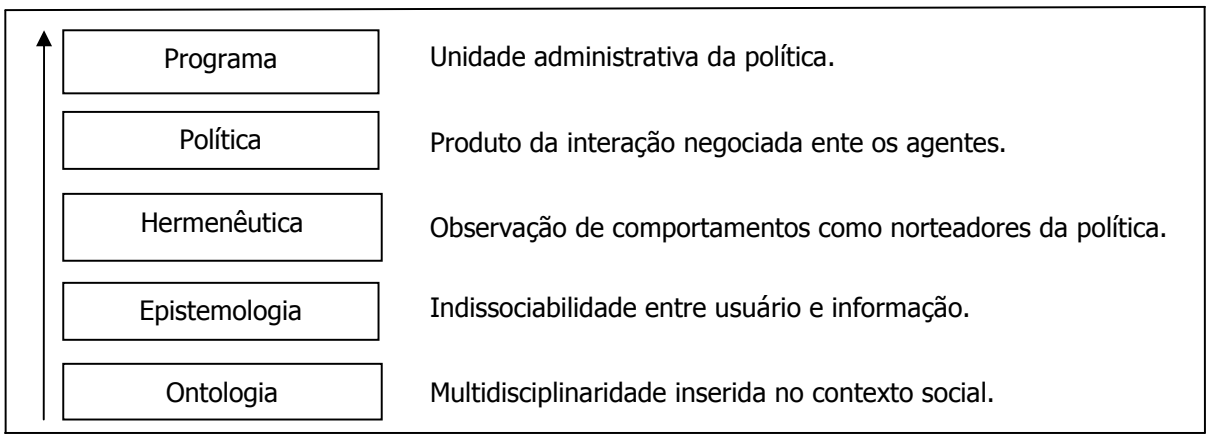
Esse trabalho teve por finalidade analisar os pressupostos para o tratamento da segurança da informação, por meio da formulação de políticas de segurança da informação, baseando-se em uma estratégia de análise fenomenológica. Tal abordagem procurou dar às políticas formuladas uma abordagem social, de caráter humanista, centrada nos pontos de vista do usuário, a fim de se contrapor aos modelos tecnicistas atuais.

Para alcançar os objetivos pretendidos, o autor utilizou os componentes fundamentais da pesquisa fenomenológica, conforme indicados por

Sanders (1982, citado por MARCIANO, 2006). O trabalho se caracterizou eminentemente qualitativo, com aspectos exploratórios, mediante o uso de diversas disciplinas para a busca de um modelo de formulação de políticas de segurança da informação, visando ao tratamento adequado dos problemas afeitos à segurança da informação.

Como resultado, propôs-se um modelo para se elaborarem políticas de segurança da informação, com base na multimetodologia. Assim, foram apresentados os pressupostos que orientaram a elaboração do modelo, sob o ponto de vista da ontologia, da epistemologia e da axiologia. A figura 1, ilustra o modelo sugerido para a formulação das políticas de segurança da informação:

Figura 1 – Estratificação para a formulação de política de segurança da informação



Fonte: Marciano, 2006.

O autor concluiu que, após a análise de diversos trabalhos sobre as políticas de segurança da informação, a maioria deles privilegia os aspectos tecnológicos. Alguns citam a importância da observação ao usuário, mas poucos tratam com profundidade a sua problematização, em moldes tais como a utilização de um modelo para apresentar as interações entre os usuários e também a interação destes com os sistemas. O autor afirma, ainda, que desconhece a existência de outros trabalhos que discutam a segurança da informação como um domínio multidisciplinar das ciências sociais e que apresentam sugestões de posturas epistemológicas para a sua abordagem.

Outro trabalho encontrado nos domínios da ciência da informação foi a dissertação defendida por Lorens (2007), no Departamento de Ciência da Informação e Documentação da Universidade de Brasília, sob o título: *Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação.*

O objetivo geral dessa dissertação foi propor um modelo para a cadeia de regulamentação dos aspectos normativos de segurança da informação e seus correlatos. Um dos objetivos específicos foi propor um modelo de integração do planejamento estratégico organizacional com o modelo da cadeia de regulamentação normativa da segurança da informação. Outro objetivo específico foi estabelecer a integração dos princípios de arquitetura da informação para o modelo proposto de cadeia de regulamentação dos aspectos normativos de segurança da informação.

O autor dividiu a pesquisa em duas partes e caracterizou a primeira como uma pesquisa descritiva analítica, construída por uma abordagem teórico-metodológica sobre um campo de conhecimento específico. Essa pesquisa foi classificada como bibliográfica por ter o objetivo de conhecer, de discutir e de analisar as contribuições registradas acerca de um tema ou de um problema. O método escolhido para a estruturação dessa primeira parte foi o da metamodelagem, conhecido como M3, proposto por Van Gigch e Pipino (1986, citado por LORENS, 2007). Esse método se sustenta em três níveis de análise incidentes sobre o objeto científico: o epistemológico, o científico e o prático.

A segunda parte constitui-se de uma pesquisa de campo, qualitativa, suportada por uma entrevista estruturada com especialistas criteriosamente selecionados, com o objetivo de captar as explicações e as interpretações do que ocorre na realidade observada. A amostra escolhida foi representada por um banco público, dois bancos mistos, um banco privado, três consultorias e um órgão público.

Assim, o autor concluiu que os modelos organizacionais de regulamentação de segurança da informação vigentes carecem de estruturação fundamentada cientificamente. Para suprir essa lacuna, propôs-se um modelo de cadeia sustentado metodologicamente, que esteja de acordo com os conceitos da

arquitetura da informação; que reflita o planejamento estratégico organizacional e que considere uma abordagem social para a segurança da informação. Segundo o autor, a pesquisa de campo permitiu identificar que a inconsistência entre os planejamentos estratégicos e os pontos de vista de segurança da informação das organizações introduzem distorções nos seus modelos normativos, tornando-os ineficientes, quando não inexequíveis.

Os pontos de vista vigentes de segurança da informação, salvo raras exceções, desconsideram ou subestimam a figura do usuário desde a sua definição, o que inevitavelmente dificulta elaborar regulamentação de segurança da informação destinada a tais usuários. O modelo de cadeia normativa para a segurança da informação proposto abrange os níveis estratégico, tático e operacional. Além disso, foram elaboradas proposições para se definirem os termos usados nesse modelo, tais como: política de segurança da informação; diretrizes de segurança da informação; normas de segurança da informação; processo organizacional de segurança da informação.

Ainda no Programa de Pós-graduação em Ciência da Informação da Universidade de Brasília, Silva (2010) apresentou a dissertação de mestrado intitulada *Gestão de Risco em Tecnologia da Informação como fator crítico de sucesso na gestão de Segurança da Informação dos órgãos da Administração Pública Federal: um estudo de caso da ECT - Empresa Brasileira de Correios e Telégrafos*.

Segundo o autor, esse trabalho caracteriza-se como uma pesquisa aplicada, pois objetiva gerar conhecimento para a aplicação dos conceitos de gestão de riscos à segurança da informação no ambiente de uma empresa pública. A abordagem utilizada teve caráter qualitativo. A base teórica que deu sustentação a esse trabalho foi construída com base em uma pesquisa bibliográfica que visou estudar os conceitos, as definições e os modelos de gestão de segurança da informação e de gestão de riscos. O universo de pesquisa foram os órgãos da administração pública federal e, em virtude da necessidade prática de selecionar uma

amostra que representasse adequadamente o universo pesquisado, escolheu-se a Diretoria de Tecnologia da ECT.

O objetivo dessa dissertação foi estudar ações que pudessem tornar mais eficiente o processo de gestão de segurança da informação, com base na aplicação do conceito de gestão de riscos, considerando-se a política, o comportamento e a cultura informacional existentes.

Dessa forma, o autor concluiu que ao tratar a questão da segurança da informação pelo viés da gestão de riscos, o gestor consegue aproximar o assunto da estratégia de negócios e empregar melhor os recursos, uma vez que ao conhecer as ameaças e as vulnerabilidades a que estão sujeitas as informações e os impactos decorrentes do comprometimento de sua segurança, a tomada de decisão para proteger os dados corporativos torna-se mais bem fundamentada e mais confiável.

No Programa de Pós-graduação em Ciência da Informação do Centro de Ciências Sociais Aplicadas da Pontifícia Universidade Católica de Campinas, consta outra dissertação de mestrado defendida por Ramos (2007), intitulada *Contribuição da ciência da informação para a criação de um Plano de Segurança da Informação*.

Esse trabalho aproxima a segurança da informação da ciência da informação e da administração e tem por objetivo dar subsídios para a criação de um plano de segurança da informação, integrado com as formas de tratamento da informação concebidas pela ciência da informação e com as técnicas de gestão utilizadas no processo de planejamento estratégico.

A metodologia utilizada foi a pesquisa bibliográfica, que consistiu em desenvolver o trabalho com base em material já elaborado, constituído, principalmente, de livros e de artigos científicos. Iniciou-se com a revisão dos conceitos de informação existentes em diversas áreas do conhecimento e a importância deles para as organizações. Em seguida, fez-se a análise do conceito de segurança da informação e sua necessidade, com base na norma que trata das práticas de segurança da informação (ASSOCIAÇÃO, NBR ISO 17799:2005). Nesse

trabalho, destinou-se um capítulo para os principais conceitos de planejamento estratégico e a descrição dos seus produtos – visão, missão, objetivos e estratégias. Destacou-se, ainda, o fluxo e a necessidade de informação nesse processo.

O autor procurou argumentar como a ciência da informação pode contribuir para a criação de um plano de segurança da informação, com base nas necessidades de informações organizacionais, na aplicação das características da informação e nos domínios de proteção, na geração de necessidade de informação qualificada e priorizada e na utilização da referida norma.

A partir das análises realizadas, o autor chegou às seguintes conclusões:

- É possível, no processo de planejamento estratégico organizacional, extrair as necessidades de informações que são geradas e organizadas em suas etapas de desenvolvimento, de execução e de controle.

- As informações podem ser caracterizadas conforme seus atributos como tipo, fonte, classificação, relevância, e também podem ser preparadas para a aplicação dos domínios de proteção.

- A qualificação e a priorização das informações são utilizadas para classificá-las de acordo com o seu nível de segurança, no contexto geral das organizações.

- A aplicação da Norma NBR/ISO 17799:2005 é resultado das necessidades analisadas, uma vez que as informações são caracterizadas para a sua aplicação.

O autor concluiu que é possível elaborar um plano de segurança da informação, uma vez que a informação foi tratada desde a sua origem no planejamento estratégico até a sua real necessidade de proteção.

Após avaliar a dissertação de Ramos (2009), constatou-se que há semelhanças entre ela e o presente trabalho. Essas semelhanças referem-se ao tratamento da segurança da informação dentro da ciência da informação e a ênfase na classificação correta da informação, visando estimar o valor da informação. Desta forma, é possível identificar a real necessidade de proteção da informação e estabelecer, com maior grau de assertividade, o nível de proteção compatível com o valor dela.

Também defendida no Programa de Pós-graduação em Ciência da Informação do Centro de Ciências Sociais Aplicadas da Pontifícia Universidade Católica de Campinas, encontra-se a dissertação de mestrado de Silva (2010), sob o título: *Gestão da Segurança da Informação: Um olhar a partir da ciência da informação*.

Essa pesquisa visava examinar a concepção de um sistema de gestão da segurança da informação - SGSI, através de dispositivos metodológicos no contexto da gestão da informação - GI, na perspectiva da ciência da informação - CI, utilizando-se o tratamento da informação no seu ciclo de vida, isto é, no contexto da coleta, da organização, do armazenamento, da recuperação e da disseminação dela. Estabeleceu-se como hipótese que os princípios da GI na perspectiva da CI podem contribuir significativamente por indicar uma abordagem sistêmica dos processos, que enfatiza as especificidades de controle (organização e tratamento), acesso e uso (representação e recuperação) na concepção de um SGSI.

O método que norteou essa pesquisa foi o indutivo. Segundo Marconi (2000, citado por SILVA, 2010), indução é um processo mental por intermédio do qual parte-se de dados particulares, suficientemente constatados, infere-se uma verdade geral ou universal, não contida nas partes examinadas. Dessa forma, o autor buscou na literatura, dados que trouxessem respostas à hipótese estabelecida.

O trabalho também adotou característica qualitativa para entender a natureza do fenômeno social estudado. O autor afirmou, ainda, que a pesquisa

também foi exploratória, pois o objetivo principal dela foi aprimorar ideias, considerando-se os mais variados aspectos relativos ao fato a ser estudado. Além disso, a pesquisa envolveu levantamento bibliográfico e análise de cenários relacionados, a fim de estimular a compreensão dela. A abordagem exploratória parte de um levantamento bibliográfico de teses, de dissertações e de trabalhos existentes nas universidades brasileiras, particularmente, os desenvolvidos nas áreas da CI, computação e administração. Pesquisou-se, também, livros e revistas especializadas, e a rede mundial de computadores para afirmar os conceitos sobre SI na CI.

Dessa forma, o autor chegou à conclusão de que a GI é a base para se fazer a administração e o gerenciamento de todos os ativos de informação, pois o objetivo dela é a obtenção, o tratamento e a organização da informação, com o intuito de fomentar a recuperação e a disseminação da informação, com economia de tempo e de recursos financeiros. Assim, a CI pode apresentar o aporte teórico conceitual das principais atividades desenvolvidas pela GI, as quais podem contribuir para o tratamento e para a organização da informação, visando salvaguardar os ativos informacionais de uma instituição e auxiliá-la na constituição do SGSI.

Visando alargar as fronteiras da presente pesquisa, buscou-se, nas mesmas bases citadas anteriormente, os seguintes termos, ainda que não guardassem ligação direta com a ciência da informação:

- Segurança da informação;
- Valor da informação;
- Pilares que sustentam a segurança da informação (tecnologia, pessoas e processos);
- Fatores que interferem na segurança da informação;
- Modelo de avaliação dos pilares que sustentam a segurança da informação.

O número de trabalhos encontrados dessa vez chegou a 730, entre teses, dissertações e artigos científicos publicados. Após a leitura deles, identificamos 159 que tinham alguma relação com os assuntos abordados no presente trabalho. Fizemos, então, uma análise comparativa com os objetivos da presente pesquisa e encontramos seis trabalhos que possuem relação com, pelo menos, um dos objetivos aqui estudados.

Menezes (2008) defendeu a dissertação de mestrado intitulada *Proposta de um modelo de avaliação da segurança da informação nas organizações centrada no usuário*, no Departamento de Engenharia de Produção da Universidade Federal de Pernambuco.

O objetivo dessa dissertação foi elaborar um modelo que pudesse oferecer subsídios às instituições, para selecionar e para analisar os indicadores de desempenho que avaliam o nível de cumprimento das diretrizes de segurança da informação por parte dos indivíduos pertencentes à organização. Essa medida visa facilitar a tarefa do gestor de TI de avaliar as condições desse cumprimento, possibilitando-lhe adotar medidas, a fim de elevar a conscientização quanto à segurança da informação, de forma que possa mostrar continuamente a conformidade com as normas da organização.

O autor classificou essa pesquisa como descritiva e comparativa. Para realizá-la consultou documentos tais como o *Building an Information Technology Security Awareness and Training Program*, elaborado pelo *National Institute of Standards and Technology – NTIS* (WILSON, 2013 citado por MENEZES, 2008), que propõe ações para se elaborar treinamento e programas de conscientização. Utilizou-se, também, a NBR ISO/IEC 27001:2006 (ASSOCIAÇÃO, 2006), no que se refere a treinamento e a punição aos usuários. Além disso, foram utilizadas pesquisas de órgãos internacionais, artigos e textos produzidos acerca do assunto.

Como conclusão, Menezes (2008) propôs a criação de um modelo que possibilitasse estabelecer indicadores básicos e suas avaliações, com vistas à

obtenção do nível de cumprimento da política de segurança. Utilizando-se de métricas sugeridas por Mathisen (2004, citado por MENEZES, 2008), foram apresentados nove indicadores que podem ser usados para medir a conscientização e o comportamento dos usuários: 1. percentual de empregados que terminaram o treinamento necessário, em segurança; 2. número de relatos de incidentes de segurança; 3. percentual de empregados que deixaram suas mesas limpas no fim do dia; 4. percentual de papel que contenha informações que, no momento de seu descarte, é fragmentado; 5. percentual de tráfego ilegal na rede interna; 6. percentual de senhas fracas de usuários; 7. número de acessos a *sites* de assuntos de segurança; 8. número de solicitações feitas ao departamento de segurança; 9. satisfação do cliente.

No Departamento de Engenharia de Produção da Universidade Federal do Rio Grande do Norte, Gabbay (2003) defendeu a dissertação de mestrado sob o título: *Fatores influenciadores da implementação de ações de gestão da segurança de informação: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte*.

O objetivo desse trabalho foi identificar quais fatores influenciam os executivos e os gerentes de TI, nas suas percepções em relação à segurança da informação. Para tanto, aferiu o nível de concordância desses executivos em relação às diretrizes da ISO/IEC 17999:2005, na sua dimensão de controle de acesso.

Segundo o autor, do ponto de vista de seus objetivos, a pesquisa pôde ser classificada como exploratória e descritiva. O método exploratório foi utilizado na fase inicial da pesquisa, visto que o objetivo maior não era o de resolver um problema, mas sim, o de caracterizá-lo. Na segunda etapa, realizou-se uma pesquisa descritiva, com o objetivo descrever o fenômeno ou a situação, mediante o estudo realizado em determinado espaço-tempo. Em relação à forma de abordagem, a pesquisa foi do tipo quantitativa; as opiniões e as informações foram traduzidas em números, as quais foram classificadas para análise por meio do uso de recursos e de técnicas estatísticas. Para realizar o estudo, e a coleta dos dados e das informações,

realizou-se uma pesquisa de campo. O universo considerado foram todas as empresas que contribuíram com ICMS no Estado do Rio Grande do Norte, em 2000. A amostra constou das 50 maiores empresas contribuintes de ICMS, no mesmo ano, naquele estado. As variáveis foram divididas em duas perspectivas, a saber: empresa e indivíduo. Para a perspectiva "empresa" foram destacadas cinco variáveis, e outras cinco foram destacadas para a perspectiva "indivíduo". Para a análise dos dados, foram utilizadas a estatística descritiva, o método de análise de agrupamento (*clusters*) e o qui-quadrado.

Através de ferramentas estatísticas, evidenciaram-se, segundo o autor, associações entre as variáveis "tamanho do parque instalado e frequência de ataques sofridos", com a variável "nível de concordância em relação à Norma NBR ISSO/IEC 17999:2005 – dimensão Controle de Acesso". Outro resultado apresentado se refere aos obstáculos para a implementação de políticas de segurança, tais como: falta de conscientização dos funcionários (56%); falta de ferramentas adequadas (41%); escassez de recursos humanos especializados (39%) e restrições orçamentárias (39%).

Por outro lado, na *Lawrence Technological University – USA,* encontra-se a tese de doutorado em Gestão de Tecnologia de Informação, defendida por Nnolim (2007), intitulada *A Framework and Methodology for Information Security Management*.

O objetivo dessa tese foi examinar como está a gestão da segurança da informação nas empresas, visando melhorá-la através da gestão de processos repetíveis. Além disso, essa tese teve ainda como objetivo desenvolver um *framework* e uma metodologia que permitisse a integração da gestão da segurança da informação com outros processos de negócio da empresa.

A metodologia de investigação adotada nesse trabalho utilizou métodos mistos, uma vez que esse foi um projeto de pesquisa centrado no problema. A estratégia utilizada foi a investigação de problemas simultâneos,

definidos como situações, nas quais o pesquisador converge dados quantitativos e qualitativos, a fim de proporcionar uma abrangente análise do problema pesquisado.

O pesquisador concluiu que ainda faltam um *framework* abrangente, um modelo de processo de suporte e uma metodologia que permitam gerir eficazmente a segurança da informação. Concluiu, também, o pesquisador que a segurança da informação não pode ser gerenciada eficazmente quando falta a maior parte dos componentes do modelo conceitual de gestão da segurança da informação. Por fim, concluiu que a gestão da segurança da informação pode ser um processo de gestão repetível, que usa uma abordagem sistemática em sua implementação.

A tese de doutorado intitulada *A model of human factors that affect organizational information security effectiveness* foi defendida por Zhang (2006) na *University of Mississippi – USA*. Nessa tese, o autor entendeu que o usuário final, parte mais importante dos sistemas de informação, tem recebido pouca atenção nos assuntos de segurança da informação. Ele ressalta que a tecnologia da informação tem se tornado cada vez mais avançada e que uma simples falha do usuário final pode se tornar um problema proeminente. Com essa visão, o trabalho discutiu como treinar e como motivar adequadamente o usuário final, para que o seu papel na segurança seja fortalecido.

O objetivo desse estudo foi determinar a significância e a importância relativa dos seguintes fatores no comportamento do usuário final nos assuntos de segurança da informação: risco percebido, intenção, atitude, norma subjetiva e controle comportamental percebido. Especificamente, esse estudo procurou responder às seguintes questões: Esses fatores interferem na determinação do comportamento do usuário final de segurança da informação? E, quais fatores são mais importantes para determinar o comportamento do usuário final?

Os dados do trabalho foram coletados usando uma pesquisa *online* e os resultados foram analisados usando a ferramenta AMOS 5.0.

Os resultados da pesquisa deram suporte à teoria de que a intenção comportamental, o controle comportamental percebido e as atitudes influenciam fortemente o comportamento dos usuários finais de segurança da informação. O pesquisador concluiu também que segurança da informação diz respeito ao negócio como um todo e não somente à tecnologia.

Segundo o autor, uma vez que o objetivo final é aumentar a efetividade da segurança da informação nas organizações, prover a tecnologia da segurança da informação pode ser o primeiro passo, mas está longe de resolver o problema de segurança. Sem o aperfeiçoamento das questões comportamentais dos empregados, é provável que as organizações nunca venham a obter a segurança adequada de suas informações.

Outro trabalho encontrado foi a dissertação de Oliveira (2009), defendida no Departamento de Engenharia de Produção da Universidade Federal de Santa Maria – RS, sob o título: Implantação de uma gestão da Segurança da Informação através da abordagem Seis Sigmas.

Essa dissertação teve por objetivo apresentar uma proposta de implantação da gestão de segurança da informação, através da abordagem *seis sigmas*, com foco nas percepções e nas expectativas dos clientes internos ou dos usuários da organização. Essa proposta visou produzir uma gestão baseada em dados concretos, a fim de promover a melhoria e a qualidade da segurança das informações.

O método DMAIC (definir, medir, analisar, implementar e controlar) foi utilizado como base para a implementação da gestão de segurança da informação. Esse método é o mais utilizado na implementação do *seis sigmas*, o qual é composto de cinco fases: definir, medir, analisar, implementar, e controlar. A pesquisa teve como princípio o foco no cliente interno ou no usuário, que é o ponto de partida para o processo de melhoria. Cada fase de execução foi instrumentada com ferramentas, com técnicas e com procedimentos, com vistas a produzir uma gestão baseada em evidências e na realidade da organização. O teste da proposta de

gestão de segurança de informação teve como cenário de aplicação as Unidades de Cardiologia Intensiva - UCI e Terapia Intensiva - UTI do Hospital Universitário de Santa Maria – HUSM.

A implantação da gestão proposta nas unidades do HUSM resultou em 22 ações planejadas para minimizar os problemas sobre a vulnerabilidade das informações. Destas, 19 foram concluídas, as quais garantiram o cumprimento das metas estabelecidas. Observou-se que o "programa de conscientização" obteve boa aceitação, uma vez que foi avaliado como "muito bom" por 72,7% dos participantes, o que contribuiu para o aumento de 43,8% da qualidade da segurança da informação, na percepção dos usuários.

Como contribuição, essa pesquisa trouxe a proposta de implantação da gestão de segurança da informação através da abordagem "seis sigmas". Tal proposta apresentou como novidade o delineamento de todas as fases de implantação estruturadas através do método DMAIC.

Proposta de adaptação do modelo Balanced Scorecard – BSC para a gestão da Segurança da Informação em órgãos da administração pública é o título de outra pesquisa sobre o assunto segurança da informação. Trata-se da dissertação de mestrado defendida por Silva (2010), na Faculdade de Tecnologia, Departamento de Engenharia Elétrica da Universidade de Brasília.

O objetivo dessa dissertação foi propor um modelo para a gestão de segurança da informação do Departamento de Segurança da Informação e Comunicação – DSIC (órgão subordinado ao Gabinete de Segurança Institucional da Presidência da República – GSI/PR). Além disso, pretendia-se que o modelo proposto pudesse servir aos órgãos da Administração Pública Federal – APF, com base na adaptação do modelo do *Balanced Scorecard – BSC*, especificamente nas perspectivas financeira e de clientes, para viabilizar a sua aplicação no setor público.

O estudo teve ainda os seguintes objetivos: identificar os relacionamentos existentes entre as perspectivas do BSC; comparar a aplicação do

BSC nos setores público e privado, a fim de identificar as limitações para a aplicação na APF; adaptar/agregar perspectivas no modelo proposto; apresentar o modelo adaptado e aplicá-lo no contexto do DSIC; e, ainda, apresentar uma solução de sala de situação estratégica como alternativa para organizar os indicadores do modelo proposto.

Trata-se de um estudo de caso realizado no DSIC. Segundo o autor, a pesquisa caracterizou-se como descritiva, pois teve como objetivo primordial descrever as características de determinada população ou fenômeno, e estabelecer reações entre variáveis. Também se caracterizou como uma pesquisa exploratória, devido à necessidade de levantamento bibliográfico e de entrevistas com pessoas que tinham experiências práticas com o problema pesquisado. Tal pesquisa configurou-se, ainda, como uma pesquisa participante, uma vez que o pesquisador era também servidor da APF. E quanto à abordagem do problema, a pesquisa foi considerada quantitativa e qualitativa.

Ao utilizar o BSC como referência de modelo de gestão estratégica a ser implementado na APF, alguns limitadores foram encontrados, notadamente em duas perspectivas: financeira e clientes.

No setor privado, a perspectiva financeira é voltada para a obtenção de lucro e para a competitividade, diferentemente do setor público que não visa lucro, posto que os recursos são destinados ao atendimento à sociedade e ao cidadão; ou seja, para a coletividade, sem qualquer tipo de competição.

Na perspectiva de clientes, como é definida na iniciativa privada, os objetivos estratégicos e as metas são direcionados para atender às necessidades de mercado e, muitas vezes, de forma personalizada. Esses fatos tratados de forma tão simples e tão eficiente no setor privado não são coerentes com as atividades da APF, pois a satisfação do cidadão/sociedade é uma obrigação do Estado e os interesses devem ou deveriam estar voltados para a coletividade.

Segundo o autor, tais características dificultaram a implantação do BSC da forma como foi desenvolvido, pelo fato de requerer adaptações e agregação de perspectivas. O pesquisador propôs as seguintes adaptações para que seja possível a implementar na APF: Desmembramento da perspectiva de clientes em Administração Pública Federal e cidadão/sociedade; adequação do nome da perspectiva "financeira" para "orçamentária"; e a criação da perspectiva "relações governamentais". Assim, a proposta da criação de um modelo de gestão estratégica para a APF, baseado no BSC apresentou seis perspectivas, a saber: aprendizado e crescimento; relações governamentais; processos internos; Administração Pública Federal; cidadão/sociedade e orçamentária.

Juntamente com esse modelo, sugeriram-se indicadores para fins de padronização das métricas utilizadas. Finalmente, elaboraram-se os mapas estratégicos nos níveis estratégico e tático, os quais definiram duas linhas de estratégias para se implementar as ações de segurança da informação na APF.

Como consequência dessa implementação, o DSIC já está utilizando a sala de situação estratégica que apresenta os indicadores das metas estabelecidas, cujos resultados são utilizados para fins de tomada de decisão quanto à gestão de segurança da informação na APF.

Os trabalhos encontrados abordam a segurança da informação sob diversos aspectos e sob diferentes óticas. Alguns deles apresentam alguma interseção com o presente trabalho. No entanto, não encontramos nenhuma pesquisa que tivesse o foco na abordagem do valor da informação e na importância de existir equilíbrio entre os pilares tecnologia, pessoas e processos, para a melhoria das ações em segurança da informação. Essa abordagem pode se apresentar como uma forma alternativa de estudo desse assunto, o que reforçou a importância e o caráter de ineditismo desta pesquisa.

4.2 Análise do referencial teórico

Contextualizado o problema no âmbito da área de estudo, ou seja, a segurança da informação na ciência da informação passou-se à análise do referencial teórico. Para tanto, identificou-se, a partir do problema, do objetivo geral e dos objetivos específicos os assuntos e os termos que deveriam ser estudados, conforme se segue:

- Informação;
- Valor da informação;
- Segurança da informação;
- Pilares que sustentam a segurança da informação;
- Modelo de avaliação da segurança da informação.

4.2.1 Informação

A informação tem sido estudada por muitos autores e é apresentada de diversas maneiras, desde redutora de incertezas até a de recurso transformador do indivíduo e da sociedade. Wersig e Neveling (1975) sistematizaram os diversos pontos de vista sobre a ciência da informação, classificando-os em quatro categorias, a saber:

- A visão orientada para o fenômeno;
- A visão orientada para os meios;
- A visão orientada para a tecnologia; e,
- A visão orientada para os fins.

As questões investigadas por esta pesquisa se enquadraram na "visão orientada para os fins", uma vez que parte do pressuposto de que existem determinadas necessidades sociais a serem preenchidas e se dedicou a desenvolver

um trabalho prático a elas relacionado. Citou-se, como exemplo, a necessidade de melhoria da segurança da informação estratégica para a gestão dos negócios de instituições bancárias, com benefícios diretos aos cidadãos correntistas bancários, não somente na proteção dos seus dados pessoais, como também na maior disponibilidade dos sistemas por eles acessados. Vários outros setores, sejam públicos ou privados, convivem com o grande problema de garantir a segurança de suas informações, fato que afeta diretamente seus clientes e cidadãos. As empresas que são obrigadas, por lei, a guardar o sigilo das informações dos seus clientes, tais como: Receita Federal (sigilo fiscal), Telecomunicações (sigilo telefônico) e bancos (sigilo bancário), têm investido vultosos recursos nessa área, sem, contudo, colherem os benefícios na intensidade esperada. As conclusões deste trabalho poderão auxiliar essas organizações a mitigar os riscos a que estão sujeitas, com vistas a melhorar a proteção das informações sob sua guarda e, dessa forma, beneficiar diretamente os cidadãos e os clientes.

Visando reduzir o problema que a ambiguidade do termo "informação" pode acarretar, por ser um termo polissêmico, os autores apontaram seis diferentes possibilidades de abordagem de "informação", com base na estrutura geral de relações entre homens e mundo, conforme a seguir:

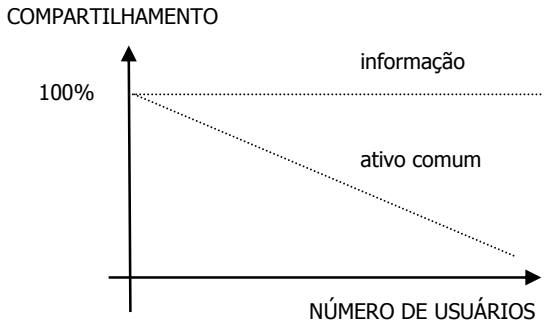
- A abordagem estrutural (orientada para a matéria);
- A abordagem do conhecimento;
- A abordagem da mensagem;
- A abordagem do significado (característica da abordagem orientada para a mensagem);
- A abordagem do efeito (orientada para o receptor);
- A abordagem do processo.

Este trabalho adotou a abordagem do conhecimento, segundo a classificação de Wersig e Neveling (1975), já que a informação aqui foi tratada como dado de valor no processo decisório. Essa é a abordagem mais aceita entre os autores que estudam a teoria da decisão, vista como o processo de preencher lacunas de conhecimento ou de informação.

Na mesma direção está o ponto de vista de Moody e Walsh (1999) para quem a informação pode ser governada por leis próprias de comportamento, e o seu valor é passível de ser mensurado. Argumentam os autores que a informação não obedece às mesmas leis econômicas dos ativos normais, por terem propriedades peculiares. Assim, propuseram sete leis para a informação, visando demonstrar suas diferentes características em relação aos demais ativos tangíveis, de modo a tornar possível a mensuração do seu valor. Os gráficos de 2 a 8 demonstram visualmente essas leis:

a) a informação é infinitamente compartilhável

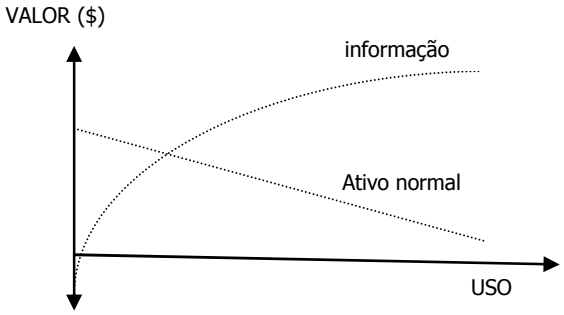
Gráfico 2 – Compartilhamento da informação



Fonte: Moody e Walsh (1999)

b) o valor da informação aumenta com o uso

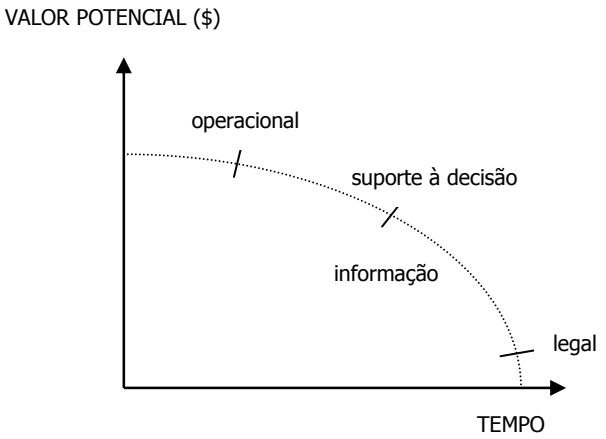
Gráfico 3 – O valor da informação com o uso



Fonte: Moody e Walsh (1999)

c) a informação é perecível

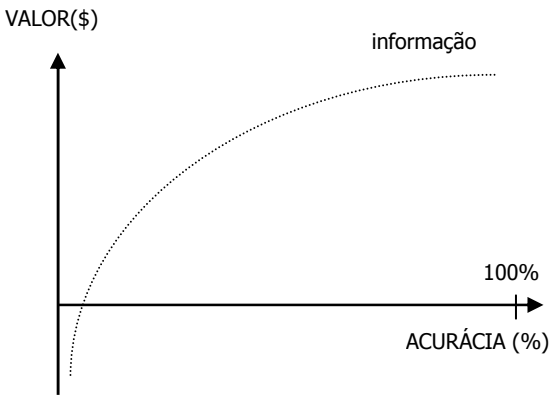
Gráfico 4 - Depreciação do valor da informação *versus* o tempo



Fonte: Moody e Walsh (1999)

d) o valor da informação aumenta com a acurácia

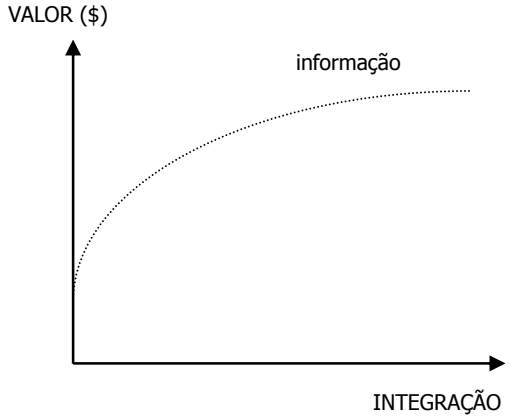
Gráfico 5 – O valor da informação com a acurácia



Fonte: Moody e Walsh (1999)

e) o valor da informação aumenta quando a informação é combinada com outra informação;

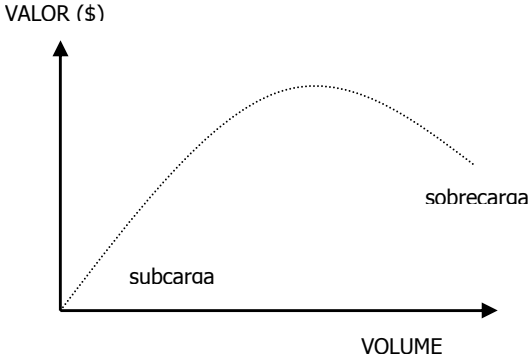
Gráfico 6 – O valor da informação com a integração



Fonte: Moody e Walsh (1999)

f) mais informação não é necessariamente melhor

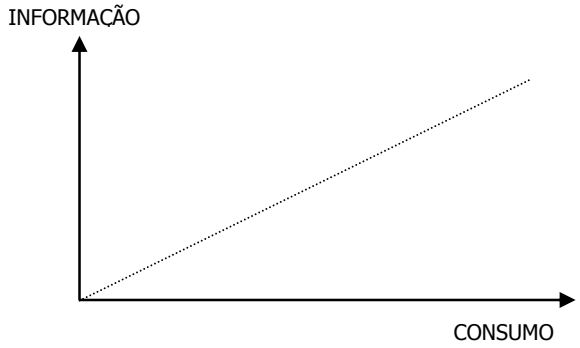
Gráfico 7 - Volume *versus* valor da informação



Fonte: Moody e Walsh (1999)

g) a informação não se esgota com o consumo: quanto mais se usa, mais se tem.

Gráfico 8 - Informação *versus* consumo



Fonte: baseado em Moody e Walsh (1999)

Esses gráficos facilitam o entendimento de que a informação pode ser analisada com base em leis próprias de comportamento, mesmo sendo um ativo intangível. Em alguns casos, verificou-se que a informação se comporta de forma contrária à de um ativo comum, mas, que é possível estimar o seu valor.

Le Coadic (2004) foi ainda mais incisivo ao afirmar que a informação tornou-se um produto, uma substância, uma matéria que adquiriu *status* de componente essencial que é o principal ativo para que as organizações desenvolvam os seus negócios.

Dias (2000), acrescenta que, além de ser o principal patrimônio da empresa, a informação está sob constante risco.

Esses pontos de vista consideram a informação praticamente como um ativo tangível. Essa é também a concepção adotada no âmbito da presente pesquisa.

4.2.2 Valor da informação

Costuma-se adotar medidas de segurança para proteger tudo aquilo que possui valor e, que, consequentemente, demanda proteção (RAMOS, 2008).

Como qualquer ativo de valor, a informação também demanda proteção. Porém, toda proteção tem um custo e, por isso, ao se determinar qual a proteção a ser dada à informação, convém que se leve em conta a seguinte expressão:

Valor da informação ≥ Custo da proteção

Para satisfazer essa expressão, é necessário conhecer tanto o valor da informação quanto o custo de sua proteção. O custo da proteção está relacionado com recursos tangíveis a serem utilizados, tais como: tecnológicos, materiais e humanos. Assim sendo, o seu cálculo, embora não seja trivial, é passível de ser estabelecido. Por outro lado, determinar o valor da informação é algo de razoável complexidade, pois se trata de atribuir valor a um ativo intangível.

Primeiramente, é necessário entender melhor o conceito de *valor*. Os economistas defendem que *valor* é aquilo que alguma coisa possui e que contribui para aumentar a riqueza. Smith[7] (1988) fez distinção entre o *valor de troca* e o *valor de uso*, o que se tornou um dos princípios fundamentais da economia. A teoria do valor de troca é mais facilmente entendida em termos monetários: as pessoas trocam dinheiro por produtos.

É muito comum aplicar-se a teoria do valor de troca, quando se analisa o custo/benefício de um projeto ou quando se implanta a solução de um determinado problema. King e Schrems (1978) definem benefício como:

> A consequência de uma ação que protege, ajuda, melhora ou promova o bem-estar de um indivíduo ou de uma organização. Benefícios assumem a forma de redução de custos, eliminação de custos, melhor desempenho operacional, melhor alocação de recursos ou algo intangível, como por exemplo, melhor compreensão de uma situação particular.

O conceito de valor de troca inclui não apenas o preço combinado entre duas partes, mas também o tempo e o esforço que um indivíduo está disposto a investir para receber os benefícios desejados. O problema para se determinar a

[7] Célebre economista inglês (1723-1790) que publicou o livro "A Riqueza das Nações (1776)" e influenciou o pensamento econômico mundial.

relação custo/benefício de um serviço de informação, ou de uma informação em si, usando apenas as propriedades da informação, é que isso pode acarretar avaliações monetárias enganosas ou inadequadas.

Para superar as limitações da teoria do valor de troca, os economistas desenvolveram um segundo conjunto de teorias chamado de valor de uso. A análise com base na teoria do valor de uso ou na teoria da utilidade volta o seu foco não para o valor monetário da informação, mas para o desejo atendido, para a utilidade, para a satisfação do usuário, para o atendimento das demandas. Assim, o valor de uma informação está relacionado com a potencialidade do seu uso, com a sua utilidade.

Seguindo essa linha de pensamento, Taylor (1986) afirmou que o valor da informação tem significado apenas no contexto da sua utilidade para os usuários. Dessa forma, o valor da informação não está associado internamente ao conteúdo da informação em si, mas externamente ao modo como o usuário percebe a informação. É uma relação entre o sujeito (usuário) e o objeto (informação). A percepção do usuário é influenciada por diversos fatores, tais como: experiências acumuladas ao longo da vida, circunstâncias e contextos em que o problema está inserido, entre outros.

Ao abordar a questão, Wersig (1993) afirmou que a percepção de si mesmo e do mundo, bem como a atribuição de valores a elementos desse mundo (informação, por exemplo) é um fenômeno informacional que, ao mesmo tempo em que influencia é influenciado pelo contexto em que se encontra o usuário. Portanto, o usuário tem papel fundamental na segurança da informação, desde o princípio do processo, já que ele é quem deve perceber e estabelecer o valor da informação.

Assim sendo, quando não se atribui nenhum valor à informação ou lhe atribuem valor inadequado, a proteção dela pode se tornar inconsistente. É como acontece na construção civil, em que para se calcular as dimensões dos pilares é preciso saber, antecipadamente, qual será a carga que terão que suportar. O cálculo começa de cima para baixo: primeiro calcula-se a carga que a laje deverá suportar

(valor da informação); depois, dimensionam-se os pilares que suportarão aquela carga (segurança da informação). Quando não se sabe qual será a carga que se colocará sobre a laje, como dimensionar os pilares? Poderão ficar super ou subdimensionados. Da mesma forma, quando não se estima o valor da informação, a proteção dela poderá ficar super ou subdimensionada. No primeiro caso, os custos com a implementação dos requisitos de proteção estabelecidos poderão ser maiores do que o próprio valor da informação e, assim, gerar gastos desnecessários. No segundo caso, os requisitos de proteção estabelecidos poderão estar aquém do valor da informação.

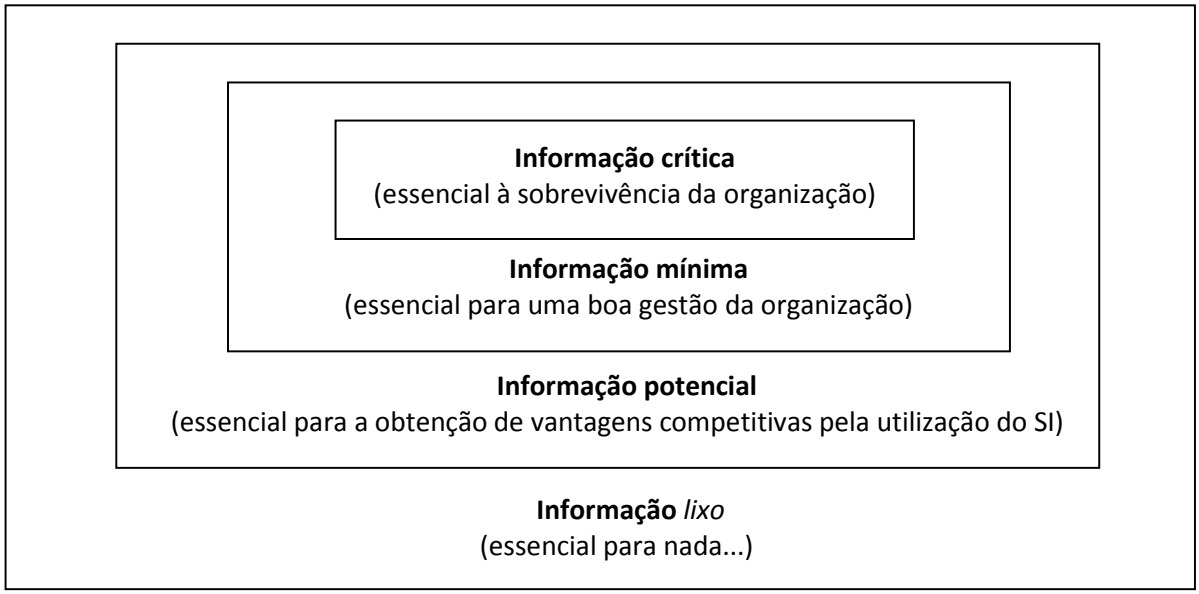
Cronin (1990) acrescentou outras duas perspectivas para se estimar o valor da informação: valor de propriedade - reflete o custo substitutivo de um bem; e, valor de restrição - que se refere à informação secreta ou de interesse comercial, quando o uso fica restrito apenas a algumas pessoas.

Na Engenharia do Petróleo, o valor da informação - VDI é uma variável muito importante e por isso é criteriosamente estudada e calculada durante as fases de avaliação, de desenvolvimento e de produção de campos de petróleo. O VDI está relacionado ao grau de incerteza presente na caracterização de um reservatório. Dunn (1992) afirmou que a informação somente tem valor, se tiver capacidade de alterar futuras decisões que possam minimizar a perda ou proporcionar ganho financeiro. Assim, segundo o autor, em situações em que a incerteza é baixa e os potenciais de perda são pequenos, o valor da informação é baixo. Por outro lado, se a incerteza e os potenciais de perda forem altos, o valor da informação será alto. Portanto, valor da informação é a validade e a relevância que a informação representa a um determinado indivíduo ou grupo.

A classificação da informação também pode trazer norteadores importantes para o equilíbrio entre o valor da informação e a proteção dela. Chaumier (1986) afirmou que a informação pode ser classificada com base nas suas finalidades, que, segundo o autor, são basicamente duas: para o conhecimento dos ambientes interno e externo de uma organização e para atuação nesses ambientes.

Baseando-se nessa classificação, Amaral (1994) propôs o desdobramento mostrado na figura 2:

Figura 2 – Classes de informação



Fonte: Amaral (1994)

Segundo Amaral (1994), a evolução do esforço por parte da organização na procura e na manutenção da informação deve ser compatível com a classificação da informação. Quanto mais crítica for a informação, mais recursos devem ser investidos na proteção dela. Quando se tratar de uma "informação *lixo*", o esforço é no sentido de se evitar qualquer dispêndio com ela.

Portanto, definir o nível de proteção que se pretende dar à informação é muito mais assertivo quando ela passa por um processo de classificação.

A forma mais comum utilizada pelas organizações para classificar as suas informações tem fundamento no conceito de Chaumier (1986). De acordo com esse conceito, leva-se em consideração a forma como as organizações se relacionam com o ecossistema em que atuam (ambiente externo) e a forma como pretendem se posicionar nesse ecossistema (ambiente interno). Assim, as informações são classificadas em estratégicas, táticas e operacionais. Essa classificação dá ideia de

valores diferentes para cada grupo de informações, o que implica diferentes níveis de proteção.

O Governo Federal classificou e estabeleceu o prazo de restrição da informação com base na lei de acesso à informação (BRASIL, 2011)

> Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.
>
> § 1o Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no **caput**, vigoram a partir da data de sua produção e são os seguintes:
>
> I - ultrassecreta: 25 (vinte e cinco) anos;
>
> II - secreta: 15 (quinze) anos; e
>
> III - reservada: 5 (cinco) anos.

Essa classificação demonstra que as diversas informações de uma organização assumem valores diferenciados, e cabe ao gestor a responsabilidade de estabelecer a proteção compatível com o valor ou com o grau de sigilo de cada grupo de informação.

Além disso, vale lembrar que o valor da informação pode se alterar ao longo do seu ciclo de vida. Assim, é preciso fazer revisões periódicas do valor da informação, para que a proteção dela não venha a se tornar inadequada. É como o arquivamento de documentos que, também, ao longo do seu ciclo de vida, passa por diferentes etapas (arquivo corrente, arquivo intermediário e arquivo permanente). Em cada momento, a informação pode assumir valores diferentes e, por essa razão, deve ser protegida de acordo com o seu valor.

Burk e Horton (1988) propuseram um método denominado *Infomapping* para gerenciar os recursos informacionais de uma organização. Porém, segundo os autores, nem toda informação pode ser considerada como um recurso. Por isso, é necessário se fazer um mapeamento para identificar quais são, de fato, as informações relevantes para a organização, para que se faça sobre elas o adequado

gerenciamento. Esse método foi concebido em quatro etapas, a saber: 1ª - mapeamento preliminar; 2ª - determinação de custos e atribuição de valor; 3ª - preparo das técnicas de mapeamento de informação; 4ª - identificação dos recursos de informação da organização.

O interesse do presente trabalho recai sobre a 2ª etapa, a qual determina os custos e atribui valor às informações. Para se determinar os custos leva-se em consideração o custo do acesso às informações, tais como criação, manutenção e atualização de banco de dados; remuneração do profissional responsável e outros custos incidentes como materiais de expediente, instalações, infraestrutura, entre outros. A etapa de atribuição de valor consiste em agregar valor às informações, fato que se fundamenta na transferência de informação como resposta intensiva a um processo humano, tanto nas atividades formalizadas, chamadas sistemas, quanto nas atividades não formalizadas. O enfoque desse critério está na relação entre os sistemas e os usuários, mediante o uso de cinco categorias, como a seguir: qualidade da informação em si, utilidade da informação, impacto na produtividade organizacional, impacto na eficácia organizacional e impacto na posição financeira.

Taylor (1986), ao considerar que a informação é uma ferramenta auxiliar no processo de tomada de decisão, propôs um modelo composto de quatro processos para agregar valor à informação, a fim de torná-la mais valiosa para o usuário. Valor agregado é o trabalho adicionado nos processos de produção de um determinado produto para atender expectativas e necessidades do usuário. Os processos propostos por Taylor são:

1. *Organização da informação* – agrega valor, pois poupa tempo na busca e na localização da informação necessária. Nas bibliotecas, é a atividade de classificar e de catalogar livros e documentos para proporcionar o acesso à informação.

2. Análise da informação – é dividida em análises voltadas para dados e para o problema. A análise voltada para dados é direcionada para o conteúdo e o

objetivo dela é mostrar a qualidade, a legitimidade e a precisão dos dados. A análise voltada para o problema é motivada pelo usuário e o seu objetivo é auxiliar o usuário a resolver um problema ou a esclarecer uma situação. Alguns processos consistem em comparar informações semelhantes e em selecionar a melhor descrição ou editar a informação.

3. Síntese da informação – consiste em reunir a informação, de uma forma significativa e ponderada, aglomerando-a em blocos que possam ser usados. Engloba a classificação do produto de acordo com a pertinência do tema, a redação de resumos executivos e a padronização da informação. A padronização é uma parte importante da síntese, porque permite a comparação de informações de fontes variadas.

4. Julgamento – é o processo final, feito por profissionais do conhecimento, que capturam a informação, sintetizam-na e padronizam-na para uma situação específica, tornando-a útil para ser usada no processo de tomada de decisão.

Essas etapas, uma vez cumpridas, agregam valor à informação sobre a qual deve pairar um novo olhar no que se refere à proteção, uma vez que, agora, o potencial de uso é maior, o que torna a informação mais valorizada.

Para Stair e Reynolds (2002), o valor da informação está diretamente ligado ao modo como a informação auxilia os tomadores de decisão a alcançar as metas de sua organização.

Como visto, existem diversas abordagens para se classificar e estimar o valor da informação. O gestor deve utilizar aquela que mais se adéqua à realidade de sua organização.

No contexto deste trabalho, valor da informação é aquilo que a informação possui e que a torna relevante em um processo de tomada de decisão. Esse valor está associado à potencialidade do uso e ao grau de sigilo da informação.

4.2.3 Segurança da informação

4.2.3.1 Breve histórico sobre segurança da informação

A segurança da informação é um assunto há muito debatido. Durante toda a história da humanidade, sempre existiram informações confidenciais, fórmulas secretas e os mais diversos interesses que não poderiam ser de conhecimento do inimigo, nem deveriam cair no domínio público. Há registro de variadas formas de segurança da informação usadas já na antiguidade para proteger informações confidenciais. A criptografia, que significa literalmente "escrita escondida", já era utilizada pelos egípcios há mais de 4.000 anos. Na Roma antiga, mensagens eram tatuadas na cabeça de escravos, que esperavam os cabelos crescerem para, então, partirem em missão. Quando eram capturados e a mensagem decifrada, os escravos, literalmente, perdiam a cabeça.

A criptografia, seja naquela época ou agora, não tem a função de impedir que informações sejam capturadas, mas de dificultar, ao máximo, a tarefa de decodificação das informações capturadas, por parte de pessoas não autorizadas.

Muitas outras formas criativas de segurança da informação foram usadas para garantir que a informação fosse revestida da confidencialidade requerida em virtude de sua importância. Ainda que não fosse reconhecida com esse nome, a segurança da informação foi algo adotado instintivamente há séculos. O que é recente não é a prática, mas o estudo sistemático da segurança da informação. Mesmo assim, o assunto remonta há mais de 70 anos. O artigo publicado por Edward Uhier Condon[8] intitulado *Science and Security* (CONDON, 1948), discute temas como a tradição da ciência em compartilhar conhecimentos, em face dos acontecimentos da Segunda Guerra Mundial e do pós-guerra, quando talvez as informações mais bem protegidas tenham sido aquelas relativas à confecção da bomba atômica. O artigo também menciona questões de equilíbrio, para que não ocorram problemas de segurança em excesso, a ponto de não se encontrar, dentro

[8] Físico nuclear americano e ex-presidente da *American Physical Society Nuclear.*

da própria organização, informações necessárias à tomada de decisão. Tal artigo aborda, ainda, questões do custo da proteção, ao se duplicar algo já feito, por receio da perda.

Com o surgimento dos computadores, a tecnologia da informação tornou-se uma grande fonte de oportunidades, mas também de riscos. Na década de 1950, os computadores eram grandes ou médios e extremamente caros. Eles eram abrigados em enormes salas com ar-condicionado, e eram operados por poucos profissionais de elevado conhecimento técnico. Não havia usuários *on-line*, nem era necessário o nome do usuário e uma senha para se ter acesso aos seus sistemas.

Segundo Landwehr (2001), nos primeiros tempos o uso da computação era basicamente em atividades militares e os problemas de segurança ficavam restritos aos acessos físicos. O foco da segurança da informação naquela época era o controle *batch* por programas individuais; o controle de acesso físico; e a manutenção de um ambiente adequado para a operação confiável do *hardware*. Problemas como interrupção de serviços, erros nos aplicativos, mau funcionamento do *hardware* eram usualmente resolvidos por profissionais da própria empresa. Essas características faziam com que os eventuais problemas de segurança fossem mais rapidamente percebidos e prontamente monitorados.

Na década de 1960, com a introdução dos computadores de menor porte, os usuários passaram a contar com computadores da companhia por meio dos chamados terminais burros, ou seja, sem capacidade de processamento local. Esses usuários, que poderiam estar fisicamente em diversos lugares na companhia, passaram a ter a possibilidade de inserir, de alterar e de apagar dados nos sistemas, porém, necessitavam ser previamente autenticados pelos sistemas, por um usuário e uma senha individual. Com a possibilidade de se compartilhar recursos computacionais, tais como a multiprogramação e o armazenamento *on line* dos registros, foi significativo o aumento do poder de processamento computacional. O número de computadores cresceu, assim como o número de usuários, de programadores e de técnicos de informática. No entanto, cresceram também as

fragilidades que causavam a insegurança nos sistemas automatizados. Com um maior número de usuários acessando *on line* os programas, os bancos de dados e outros arquivos, surgiu a preocupação com a proteção das informações contra erros inadvertidos ou intencionais.

Em 1970 foi publicado nos Estados Unidos, o documento *Security Control for Computer System: Report of Defense Science Board*, com a participação do *Department of Defense* - DoD e da *Central Intelligence Agency* - CIA. Esse documento estabeleceu um conjunto de regras que deviam ser observadas quanto à segurança da informação (SECURITY, 1970).

Ainda na década de 1970, dois eventos mereceram destaques na história da computação: o desenvolvimento dos microprocessadores e das tecnologias de rede. Com a chegada dos microcomputadores, a preços bem mais acessíveis do que os computadores da década de 1960, muitas empresas e mesmo pessoas físicas puderam adquirir seus equipamentos, e os sistemas automatizados, notadamente na área administrativa, foram largamente difundidos no mercado. Naquela época, os microcomputadores eram *stand-alone*[9]. Nesse caso, esses primeiros equipamentos pessoais não impactaram significativamente a segurança dos sistemas centrais de informação.

Outro evento importante foi o desenvolvimento das tecnologias de rede. A primeira rede nacional desenvolvida nos Estados Unidos foi a ARPANET - *Advanced Research Projects Agency Network*, no final de 1969. Tratava-se de uma rede simples que tinha apenas quatro nós. Os computadores foram interconectados por intermédio de linhas telefônicas dedicadas. A novidade foi que, pela primeira vez, os sistemas computacionais foram acessados de fora da empresa, e ficaram expostos ao mundo exterior. Desde então, tornou-se possível interagir com outros computadores, de qualquer lugar físico. Com a expansão das redes e dos terminais remotos, os controles de segurança com foco apenas no acesso físico a salas de computadores já não eram suficientes. Em resposta às novas vulnerabilidades, foram

[9] Equipamento que não fica ligado a nenhuma rede e é controlado unicamente pelo próprio usuário.

desenvolvidos sistemas de controle de acesso lógico, para permitir que somente usuários autorizados, autenticados pelos sistemas, pudessem acessar os recursos computacionais. Com um volume grande de sistemas automatizados, percebeu-se que a indisponibilidade deles poderia impactar negativamente os negócios das empresas. Dessa forma, cresceu a preocupação com a rápida recuperação dos recursos computacionais, quando ocorressem eventos que pudessem tornar máquinas e sistemas indisponíveis e, até mesmo, corromper dados. Assim, como medida de segurança, as organizações começaram a implementar os planos de contingência ou de recuperação de desastre.

Durante a década de 1980, os computadores pessoais se consolidaram e grande parte da população passou a ter acesso a eles. O rápido crescimento das aplicações para escritório, como os processadores de texto, as planilhas eletrônicas, os sistemas de pessoal, de contabilidade e de patrimônio, aliado ao baixo custo do *hardware*, permitiu que milhares de microcomputadores fossem instalados em casas, em escritórios, em indústrias e em instituições governamentais. Cada vez mais exigentes, os usuários queriam a facilidade de compartilhar aplicativos e dados entre eles, o que era ainda de difícil solução. Para atender essas necessidades, os técnicos desenvolveram as chamadas LAN - *Local Area Network*, que possibilitaram o desejado compartilhamento de aplicativos e de dados, embora ainda fosse limitado somente aos sistemas baseados em uma rede local de computador. O servidor e as estações de trabalho (terminais) em uma LAN estavam, na maioria das vezes, equipados com *modems* que permitiam que usuários remotos acessassem uma LAN através de uma linha telefônica discada e, então, compartilhassem o desejado. Isso foi um grande avanço, porém, por outro lado, outras vulnerabilidades foram expostas e fizeram com que se intensificasse a discussão sobre as questões de segurança da informação. Como desdobramento dos debates, o DoD editou o documento *Trusted Computer System Evaluation Criteria* (ESTADOS UNIDOS, 1985), que ficou mais tarde conhecido como *The Orange Book.* Esse documento consistiu em um conjunto de regras que deveriam ser utilizadas no processo de avaliação da segurança. Além disso, tal documento estabeleceu critérios

para se estipular níveis de segurança recomendados. Em uma iniciativa semelhante, o governo britânico criou, em 1987, o *Commercial Computer Security Centre – CCSC* e em 1989 foi publicada a primeira versão do "PD0003 – Código de Gerenciamento de Segurança da Informação". Esse documento estabeleceu critérios para a avaliação da segurança da informação e definiu um código de segurança para os usuários de informações (REINO UNIDO, 2013).

A década de 1990 pode ser considerada como a era da interconectividade. Com o aumento da popularidade das LANs, o desenvolvimento das WANs (*Wide Area Networks*), o surgimento de aplicações comerciais para a internet e *World Wide Web*, a interconexão de computadores tornou-se definitivamente possível e viável. Muito rapidamente, a internet e a *World Wide Web* se tornaram grandes instrumentos utilizados globalmente pelas redes de trabalho. O amplo acesso provido pela internet criou uma nova oportunidade para as organizações se comunicarem com seus clientes e com seus fornecedores. O cliente passou a poder acessar livre e diretamente um *Website* de seu interesse, obter informações sobre produtos, fazer perguntas e, por fim, realizar a compra desejada, tudo virtualmente. Essas transações comerciais via internet, ficaram conhecidas como *e-commerce*, as quais têm movimentado bilhões de dólares no mercado mundial. No entanto, muitas vulnerabilidades foram identificadas nos componentes das plataformas do *e-commerce*. O Código de Gerenciamento de Segurança da Informação – PD003 (1989) foi aperfeiçoado, passou por algumas revisões e foi homologado pela *International Organization for Standardization – ISO*, em 2000, com a denominação ISO/IEC 7799:2000 (INTERNATIONAL, 2005).

Já no início deste século XXI, a tecnologia da informação está presente não apenas nos *desktops, notebooks, smart phones*, mas em todo lugar. A comunicação, de maneira geral, seja entre clientes e fornecedores, seja entre colaboradores de uma mesma empresa, tornou-se ampla, irrestrita, rápida e, praticamente, ilimitada. Usuários podem acessar seus dados e seus sistemas de qualquer lugar do mundo. De acordo com as previsões no *Mobile World Congress* (2010), que é o maior evento de tecnologia móvel do mundo, as pessoas vão usar

mais equipamentos portáteis *wireless* para se conectarem à internet (*notebooks, tablets, smart phones*, dentre outros) do que computadores pessoais do tipo *desktops*, já em 2012. Porém, quanto mais a tecnologia evolui, mais avançam as técnicas para se obterem lucros por meio do roubo de informações alheias. Nessa guerra, o principal alvo passou a ser as informações que trafegam na internet e são armazenadas nos meios eletrônicos. Nessa área, os fraudadores aproveitam para obter seus lucros.

Nesse cenário, a segurança da informação tem se tornado de alta complexidade e, na maioria das vezes, está um passo atrás daqueles que fazem do roubo de informações um desafio a ser constantemente superado. Assim, a segurança da informação deve estar, obrigatoriamente, na agenda dos administradores; deve fazer parte do cotidiano e das estratégias das empresas e deve estar, ainda, em contínuo processo de evolução, para que as informações possam ser adequadamente protegidas.

Para atender a essa necessidade, em 2005 e em 2007, revisou-se a principal norma de segurança da informação, a ISO/IEC 7799 (INTERNATIONAL, 2005), que passou a denominar-se *ISO/IEC 27.002 – Information Technology – Security Techniques – Code Of Practice For Information Security Management.*

O Brasil tem seguido as normas da *International Organization for Standardization – ISO*, que são publicadas pela Associação Brasileira de Normas Técnicas – ABNT. Trata-se, basicamente, da tradução da norma acima mencionada, com algumas adaptações da ISO/IEC 7799, que assumiu a sigla NBR ISO/IEC 17799 (ASSOCIAÇÃO, NBR ISO/IEC 17799, 2005) e, posteriormente, NBR ISO/IEC 27.002:2005. *(*ASSOCIAÇÃO, NBR ISO/IEC 27.002, 2005).

4.2.3.2 Definições e termos de segurança da informação

O conceito de segurança da informação ainda está em processo de consolidação, e há na literatura várias definições que o abordam com diferentes focos, em diferentes contextos.

A NBR ISO/IEC 27.002:2005 define segurança da informação como *a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio* e estabelece como objetivo da segurança da informação *a preservação da confidencialidade, da integridade e da disponibilidade da informação* (ASSOCIAÇÃO, NBR ISO/IEC 27.002, 2005).

Esses termos estão assim definidos na NBR ISO/IEC 27.001:2006 (ASSOCIAÇÃO, NBR ISO/IEC 27001, 2006):

- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- Integridade: propriedade de salvaguarda da exatidão e completeza de ativos;
- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Também consta dessa norma que, além da preservação da confidencialidade, da integridade e da disponibilidade, outras propriedades podem fazer parte desse conjunto integrado que constituem a segurança da informação, tais como: autenticidade, responsabilidade, não repúdio e confiabilidade. No entanto, a importância relativa dessas propriedades ainda é motivo de controvérsia entre os estudiosos da segurança da informação. Esses termos não foram definidos na norma, mas foram encontradas as seguintes definições, no contexto da segurança da informação:

- Autenticidade: propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de alterações ao longo de um processo. Segundo o Tribunal de Contas da União (TRIBUNAL, 2008), a autenticidade assegura a correspondência entre o

autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

- Não repúdio ou irretratabilidade: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação feita anteriormente.

- Confiabilidade/Credibilidade (reliability): habilidade em prestar o serviço prometido com confiança e precisão (COOK, 2000). Na engenharia de *software*, confiabilidade é a capacidade do produto de *software* manter um nível de desempenho especificado, quando usado em condições especificadas (ASSOCIAÇÃO, 2003).

Embora a norma não estabeleça hierarquia entre os objetivos de controle, dependendo do caso, pode-se perceber maior relevância de um sobre os outros. Por exemplo, nas aplicações de comércio eletrônico ou bancárias, a disponibilidade tem sido o item mais requerido pelos usuários.

Vários autores propuseram definições para a segurança da informação e estudaram suas características:

- Zapater e Suzuki (2005) afirmaram que a segurança da informação pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associadas aos diversos ativos informacionais de uma corporação, independentemente da forma ou do meio em que são compartilhados ou armazenados.

- Summers (1997) definiu segurança da informação como uma componente conjugada ao uso de computadores e a considerou uma meta a ser atingida, para proteger os sistemas computacionais contra ameaças à confidencialidade, à integridade e à disponibilidade.

- Para Sêmola (2003), segurança da informação é uma área do conhecimento dedicada à proteção de ativos de informação contra

acessos não autorizados, contra alterações indevidas ou contra sua indisponibilidade.

- Segundo Peltier (2001), segurança da informação compreende o uso de controles de acessos físicos e lógicos para os dados, a fim de garantir o uso apropriado desses dados e impedir modificações acidentais ou não autorizadas, destruição, quebra de sigilo, perda ou acesso aos registros e aos arquivos, de forma manual ou automaticamente, bem como perdas, danos ou mau uso dos ativos informacionais.

- Na definição de McDaniel (1994), segurança da informação é o conjunto de conceitos, de técnicas e de medidas técnicas e administrativas usadas para proteger os ativos informacionais contra obtenção, dano, revelação, manipulação, perda ou uso não autorizados, deliberada ou inadvertidamente.

- O Dicionário de Biblioteconomia e Arquivologia (CUNHA e CAVALCANTI, 2008) define segurança da informação como um conjunto de procedimentos para a proteção do acervo informacional de uma organização contra acesso, ou uso por pessoas não autorizadas. Essa proteção é caracterizada pela preservação da: a) confiabilidade; b) integridade; c) disponibilidade.

Ao observar que a maioria dos autores deixou de abordar o fator humano e o enfoque social em suas definições de segurança da informação, Marciano (2006) argumentou que não se conhece qualquer solução meramente tecnológica para problemas sociais. E complementa afirmando que, por se tratar de um conceito eminentemente social, a segurança da informação necessita de uma visão igualmente embasada em conceitos sociais, além dos tecnológicos, para a sua correta cobertura.

Outro ponto de vista é o do *INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE* (2006) que concebeu a segurança da informação não

apenas como uma questão tecnológica, mas como uma questão do negócio e, que, por essa razão, envolve uma apropriada gestão de riscos para proteger adequadamente a informação em todos os níveis da organização.

Por reconhecer a pouca efetividade das soluções correntes de segurança da informação, os pesquisadores Krause e Tipton (1999) sugeriram que os requisitos de segurança sejam integrados no desenvolvimento do ciclo de vida dos sistemas de informação. Eles defenderam a ideia de que as questões de segurança sejam consideradas em todas as fases do desenvolvimento de sistemas e não somente na fase pós-implantação.

Por outro lado, Landwehr (2001) apontou algumas questões, ainda não satisfatoriamente resolvidas, relacionadas ao desenvolvimento de sistemas, tais como: práticas de programação inseguras; decisões de projeto inseguras, particularmente na camada de aplicação; arquitetura de sistemas complexa e difícil de gerenciar.

A preocupação com a segurança deve existir durante todas as fases do ciclo de vida da informação, com soluções simples e inteligentes, para que as organizações possam se apresentar ao mercado de maneira segura, pois a insegurança gera medo e o medo pode inibir novas conquistas.

Considerando-se as diversas definições acerca da segurança da informação, percebeu-se que elas são complementares em suas abordagens. Dessa forma, para efeito deste trabalho, a segurança da informação não foi vista como de responsabilidade única da tecnologia; pelo contrário, a tecnologia sozinha é incapaz de solucionar a questão. A segurança da informação foi vista como de responsabilidade do negócio, o que requer que todas as áreas da organização se envolvam com o problema. Nesse sentido, é preciso que se considere o ser humano como fator relevante para o resultado das ações de segurança da informação.

Por outro lado, sabe-se que segurança absoluta não existe, ainda que se façam investimentos vultosos nessa área. Os perímetros de segurança, ainda

que bem definidos, serão eventualmente ultrapassados; pessoas autorizadas, mesmo que não intencionalmente, podem cometer erros; problemas de desonestidade podem ocorrer e, até mesmo, de vingança de empregados ou de ex-empregados insatisfeitos; processos, ainda que bem desenhados, podem ser descumpridos. Enfim, alguma violação poderá ocorrer. A segurança da informação, portanto, não visa estabelecer segurança total, mas sim, identificar as vulnerabilidades de um processo, gerenciar os riscos decorrentes disso e mitigar o impacto, caso algum desses riscos se concretize.

4.2.4 Pilares que sustentam a segurança da informação

Quanto aos componentes principais ou pilares que sustentam a segurança da informação, adotou-se a concepção de Pfleeger (1997), para quem o investimento em segurança da informação deve ter como base três segmentos: pessoas, tecnologia e processos. Laudon e Laudon (2007) afirmaram que, para proteger sistemas de informação contra acesso não autorizado, uso indevido, destruição ou adulteração de ativos, é necessária uma combinação entre treinamento, procedimentos e tecnologias.

Para Stair e Reynolds (2002) e O'Brien (2001), um sistema de informação é uma série de elementos ou de componentes inter-relacionados, formados por pessoas, processos e recursos de tecnologia da informação. Esses componentes coletam (entrada), manipulam e armazenam (processo), disseminam (saída) os dados e as informações, a fim de produzir informações relevantes e precisas, para disponibilizá-las às pessoas certas, em tempo hábil. Além disso, fornecem, finalmente, um mecanismo de *feedback*. Para que se possam proteger os sistemas de informação, devem-se promover ações que cubram todas as dimensões desses sistemas: pessoas, processos e tecnologia.

O pilar que, historicamente, tem recebido maior atenção e maior investimento é a tecnologia. Porém, segundo Marciano (2006), a tecnologia é capaz de apresentar parte da solução a esse problema, embora não seja capaz de resolvê-lo integralmente, inclusive, em alguns casos, contribui para agravá-lo. Para o autor,

que a segurança da informação é um fenômeno social e, nesse sentido, outros fatores, como pessoas e processos, interferem diretamente na eficácia da segurança da informação. Por essa razão, necessitam ser cuidadosamente estudados.

Entre abril e junho de 2006, a Ernst & Young[10] conduziu uma pesquisa intitulada Pesquisa Global sobre Segurança da Informação 2006 (ERNST, 2006), com executivos de aproximadamente 1.200 organizações globais e agências governamentais, sem fins lucrativos. Essa pesquisa foi feita em 48 países, a qual constatou que, nos últimos anos, houve significativos investimentos em segurança da informação, que incluem não somente tecnologia, mas também pessoas e processos, com ênfase nestes últimos. Além disso, tal pesquisa revelou que esses pilares são fundamentais para a proteção da informação e que devem ser cuidadosamente balanceados de acordo com a relevância de cada um, na proporção do valor da informação.

A seguir, são detalhados os três pilares.

4.2.4.1 Tecnologia

Em fevereiro de 2007, a revista Exame (CESAR, 2007) publicou que, naquele ano, pela primeira vez na história, a expectativa era de que se venderiam mais computadores do que aparelhos de TV. Atualmente, não somente a venda de computadores é muito superior a de TV como também em 2013 a venda de *tablets* já havia superado a venda de *desktops* (IDC, 2013). Em outras palavras, isso significa que, o que antigamente era acessível somente às classes mais favorecidas, agora contempla a maioria dos lares brasileiros.

No meio corporativo, a adoção de tecnologia não é uma questão de opção, ela é indispensável no dia a dia. É praticamente impossível se pensar hoje em uma corporação que não use intensamente a tecnologia. Mesmo assim, a tecnologia ainda é vista por muitos de forma desconectada, separada do negócio; apenas como uma ferramenta de suporte. Porém, a dependência que a área de negócio passou a

[10] Empresa multinacional de auditoria e consultoria.

ter da tecnologia se tornou algo tão forte que a falta ou a indisponibilidade dela, geralmente, acarreta elevados riscos para o sucesso das empresas.

Segundo Baltzan e Phillips (2012), a confiabilidade e a solidez dos sistemas de tecnologia da informação nunca foram tão essenciais para o sucesso dos negócios. Qualquer interrupção nos sistemas críticos de TI para o negócio pode causar prejuízos em um curto intervalo de tempo, seja reduzindo receitas ou elevando despesas. Os efeitos vão desde a queda de faturamento, a diminuição da carteira de clientes, o impacto negativo na imagem institucional até multas contratuais. No caso de segmentos muito regulamentados, podem, inclusive, comprometer a permanência da empresa no mercado.

Muitos administradores, numa visão mais atual, entendem que a tecnologia não apenas dá suporte ao negócio, mas, que é parte dele. O uso eficaz da TI e a integração entre sua estratégia e a estratégia do negócio vão além da ideia de ferramenta de produtividade; é, muitas vezes, fator crítico de sucesso (LAURINDO, 2001). Em várias empresas, o gasto com tecnologia não é mais considerado uma despesa e sim um investimento. Assim, o planejamento em tecnologia precisa estar alinhado aos objetivos e aos resultados de negócios. Dessa forma, devido ao fato de a tecnologia estar tão presente no negócio, os gerentes de negócio precisam conhecer de tecnologia e, igualmente, os gerentes de tecnologia precisam conhecer do negócio.

Essa nova realidade rompe as barreiras entre a gestão do negócio e a área de tecnologia, e impacta fortemente os aspectos que compõem a tecnologia da informação. Por exemplo, os riscos e as oportunidades de TI são também riscos e oportunidades de negócio. Isso significa que, se a TI de uma empresa não vai bem, dificilmente o resultado do negócio dessa empresa será satisfatório. Consequentemente, o gerente de tecnologia passa a ser cobrado não somente pela entrega de um nível satisfatório de serviço de TI, mas também pelo gerenciamento de riscos, pela redução de despesas e por outras atividades que possam representar melhoria do resultado do negócio.

A vantagem competitiva das organizações está intimamente ligada às suas informações estratégicas e, a maioria delas está sendo gerada, armazenada, disponibilizada e comunicada mediante o uso de tecnologia.

O paradoxo é que a mesma tecnologia que tem tornado o acesso à informação cada vez mais simples, também o torna cada vez mais perigoso. A busca pela mobilidade e pela convergência, que traz grande benefício como a facilidade na execução de processos e a comodidade do usuário, hoje se tornou uma preocupação para os profissionais da informação. Ferramentas como *notebooks, pen drives, iPads, MP3 players*, máquinas fotográficas digitais, *smart phones, tablets* e assemelhados facilitam muito o acesso e o armazenamento da informação, mas exigem políticas específicas de segurança muito mais eficazes.

Diariamente, criam-se ferramentas para gerenciar o acesso a conteúdos específicos, para bloquear a instalação de códigos nas redes corporativas, o que demonstra que a preocupação com a proteção da informação cresce em proporções semelhantes ao aparecimento de novas tecnologias, porque uma nova facilidade pode ser também uma nova fragilidade. Isto é, por mais inteligentes que sejam as redes de computadores, elas ainda continuam muito vulneráveis a erros e a sabotagens.

Diante desse ciclo vicioso, o investimento em tecnologia continua sendo uma ação de alta relevância, que é determinante para a proteção das informações. Nos cenários econômicos globalizados de hoje, a implementação de políticas de segurança da informação, num ambiente de tecnologia da informação, é condição *sine qua non* para o processo de gerenciamento estratégico de qualquer organização (IMONIANA, 2004). A escolha adequada da infraestrutura de TI é fundamental para se estabelecerem padrões de segurança satisfatórios, que sejam executados discretamente em segundo plano; que tenham o menor impacto possível no desempenho dos processos de negócio e que sejam suficientemente consistentes para proteger as informações estratégicas.

Uma análise completa deve ser feita periodicamente em todo o ambiente de tecnologia, visando mapear as vulnerabilidades existentes. Essa análise deve ser acompanhada de um plano de ações para corrigir tais vulnerabilidades, uma vez que a segurança da informação está diretamente ligada à segurança de TI, que pode ser obtida somente por intermédio de um competente gerenciamento de risco. O desafio é encontrar o equilíbrio entre a facilidade de uso, o desempenho das aplicações e a segurança requerida. Essa é a principal função do pilar *tecnologia*.

4.2.4.2 Processos

Outro fator muito importante para sustentar a segurança da informação é o pilar *processos*. Grande parte dos incidentes de segurança ocorre exatamente em virtude de vulnerabilidades nos processos. Isso é o que demonstrou a pesquisa realizada pela Symantec[11] do Brasil, denominada *Relatório sobre Gerenciamento de Risco à Tecnologia da Informação Volume II* (Symantec, 2008). Segundo essa pesquisa, assuntos referentes a processos causam 53% dos incidentes de TI. Além disso, 65% das empresas entrevistadas afirmaram que não possuem processos, nem procedimentos, nem metodologia formalizada para a análise do risco a que suas informações estão sujeitas.

Segundo Hammer (1998), tradicionalmente, as empresas ignoram seus processos, mas têm muito a ganhar ao se dedicarem a conhecê-los melhor, pois todo trabalho importante que se realiza ou todo produto ou serviço oferecido por uma empresa faz parte de algum processo.

Processo, na definição de Hammer e Champy (1994), é um grupo de atividades realizadas numa sequência lógica, com o objetivo de produzir um bem ou um serviço que tem valor para um grupo específico de clientes. A NBR ISO 9001:2000 (ASSOCIAÇÃO, 2000) define processo como um conjunto de atividades inter-relacionadas que transformam insumos (entrada) em produtos (saídas).

[11] Empresa de origem americana, especializada em aplicações de segurança da informação, proprietária do antivírus Norton.

Os processos de negócio são ligados à essência do funcionamento da organização, por isso é tão importante conhecê-los. Eles são próprios de cada empresa e são muito diferentes de uma organização para outra.

Identificar o processo como a maneira típica de realizar um trabalho é importante para definir a forma básica de organização das pessoas e dos demais recursos da empresa (DREYFUSS, 1996).

Para proteger suas informações, é indispensável que uma organização defina muito bem os seus processos de negócio e faça o mapeamento das respectivas fragilidades. Os incidentes de segurança ocorrem sempre a partir de fragilidades. Conhecendo os processos e suas fragilidades, a empresa pode implementar melhorias, criar valor, fortalecer sua estratégia de atuação e, ainda, preparar uma série de ações (respostas) antecipadas, visando reduzir o impacto em caso de incidente.

Processos mal definidos, burocráticos ou fragmentados acarretam confusão e resultam em pouca eficiência nos negócios da empresa. A tecnologia pode ajudar muito no estudo, na automatização dos processos empresariais e influenciar tanto na forma de realizar o trabalho como na maneira de gerenciá-lo. No entanto, é preciso ter cuidado para não deixar tudo por conta da tecnologia, que apenas automatiza o que os analistas desenham. Vale lembrar que, na década de 1990, os analistas de processo foram desaparecendo do mercado, devido à promessa de que os processos seriam automatizados e que seus fluxos ficariam definidos nos próprios sistemas. Passados alguns anos, os analistas de processos estão sendo chamados de volta para ajudar na tarefa de organizar aquilo que, em determinado momento, pareceu que poderia ser resolvido com pura tecnologia.

A importância de se empregar o conceito de processo tem aumentado, principalmente nas empresas que trabalham com conteúdo mais intelectual, com o objetivo de oferecer produtos com alto percentual de valores intangíveis agregados. Muitas organizações estão abandonando a estrutura por funções, que foi a forma organizacional predominante nas empresas do século XX, e

estão organizando seus recursos e seus fluxos a partir de seus processos de negócio. A lógica de funcionamento está passando a acompanhar a lógica desses processos, e não mais o raciocínio compartimentado da abordagem funcional. Segundo Hammer (1996), a organização orientada para processos está surgindo como a forma organizacional dominante no século XXI.

Outra questão que merece atenção especial é o fato de as organizações estarem cada vez mais voltadas a satisfazerem as necessidades explícitas e implícitas do mercado. Nesse aspecto, um dos principais desafios a ser superado é identificar o que o cliente quer, em face de tantas mudanças, e, além disso, priorizar os processos que agregam valor, considerando esse cenário evolutivo. Esses processos devem ser gerenciados de forma especial, revestidos da proteção compatível com o valor que representam.

Davenport (2004) atribuiu o sucesso das empresas japonesas, nas décadas de 80 e 90, frente às suas concorrentes americanas, ao fato de terem descoberto e implementado o gerenciamento de processos. Por entenderem a importância do gerenciamento de processos, muitas empresas daquele país desenvolveram processos rápidos e eficientes em áreas-chave como desenvolvimento de produtos, logística, vendas e comercialização.

Processos bem desenhados e otimizados, não apenas aumentam a eficiência hoje, mas também criam chances de melhor desempenho no futuro. Ao aprimorar a capacitação organizacional, novos produtos podem ser desenvolvidos de forma mais rápida e com maior qualidade.

Devido à grande importância que os processos têm para as organizações é que eles se tornaram um dos fatores fundamentais para as ações de segurança da informação. Não é possível proteger as informações de alto valor agregado para as organizações, sem o adequado gerenciamento dos seus processos de negócio.

4.2.4.3 Pessoas

As empresas continuam a planejar sistemas de informação complexos e caros que não podem funcionar a não ser que as pessoas modifiquem o que fazem (DAVENPORT, 1998). Esse mesmo autor acrescentou que só a tecnologia não basta para o sucesso na era da informação. É preciso que o ser humano seja considerado nessa equação, em suas dimensões individuais e sociais, pessoais e transcendentes.

Saracevic (1996) abordou a questão do ser humano nas relações homem-máquina, argumentando que o lado tecnológico dessa equação está em contínua expansão. Esse fato torna o equilíbrio da equação mais difícil, de tal forma que é mais fácil adaptar o humano ao sistema do que vice-versa. Ou seja, em vez de a tecnologia se adaptar ao homem, a situação foi invertida, causando certa revolta do usuário, que, muitas vezes, até mesmo por defesa, resolve ignorar aquilo que julga não ser relevante. Para a segurança da informação, essa revolta pode se tornar perigosa, quando ocorre uma análise equivocada daquilo que parece ou não ser relevante. O pilar *pessoas,* por ser o mais frágil e, exatamente por essa razão, o mais visado pelos fraudadores, carece de maior atenção e de mais estudo.

De acordo com a 10ª Pesquisa Nacional de Segurança da Informação, conduzida pela Módulo[12] (2006), com 600 profissionais de segurança da informação de organizações privadas, públicas e de economia mista, apenas 18% declararam que possuem pessoal plenamente capacitado para atuar na área de segurança da informação. Quando consultadas se os empregados estão conscientizados sobre a importância da segurança da informação, somente 55% delas disseram que sim.

O que se observou é que o elemento humano ainda é pouco considerado como um fator decisivo para a implementação de boas práticas de segurança da informação. Na direção contrária, as pesquisas mostram que os

[12] Fundada em 1985, a Módulo é uma empresa brasileira, com atuação internacional, especializada em soluções para Governança, Riscos e *Compliance*.

principais incidentes de segurança são originados dentro das próprias empresas, por empregados, por ex-empregados ou por terceiros insatisfeitos, ou ainda, por empregados de boa-fé que são vítimas de pessoas bem preparadas, que se utilizam da engenharia social para conseguirem informações confidenciais da empresa que é o alvo do ataque.

As pesquisas em segurança da informação, geralmente estão centradas nos aspectos técnicos da segurança da informação e, muitas vezes, ignoram a dimensão humana (STANTON, 2003). No entanto, concentrar-se apenas nos aspectos técnicos e nos aspectos processuais de segurança da informação é insuficiente, porque os usuários podem, simplesmente, não seguir as determinações de segurança estabelecidas. Quando isso ocorre as medidas de proteção das informações se tornam inócuas. Consequentemente, do ponto de vista da eficácia das ações de segurança da informação, o que se requer é que os usuários estejam cientes do seu papel e o cumpram integralmente. Por isso, Pipkin (2000) considerou que um programa de conscientização é o primeiro passo para a segurança da informação.

Por considerar o fator humano relevante nas ações de melhoria da segurança da informação, tanto a comunidade científica quanto os profissionais da área de segurança passaram a investigar essa relação. Puhakainen (2006) relacionou vários trabalhos (anexo 1) propostos por essas comunidades, voltados para o estudo do comportamento do usuário e como conscientizá-lo sobre a importância de seu papel na segurança da informação.

As abordagens desses estudos estão basicamente voltadas para a conscientização do usuário, visando despertar atenção dele para as questões de segurança e mostrar-lhe que é o seu comportamento que define, na maioria das vezes, a eficácia de todo um programa de proteção da informação. Ao falarmos de segurança da informação, estamos falando, obrigatoriamente, do comportamento das pessoas que lidam com informações.

Estabelecer uma política de segurança da informação (PSI) pode solucionar parte dos problemas relacionados à segurança, mas não pode resolvê-los integralmente, porque os recursos humanos, presentes no ambiente interno das organizações, podem comprometer seriamente a efetividade de uma PSI (ELLWANGER, 2009). Não importa quão bem projetada seja a PSI, ela depende de indivíduos para implementá-la. Isso significa que o fator humano tem que ser considerado como decisivo para a implementação de boas práticas de segurança da informação, embora seja o elo mais fraco e mais complexo da corrente, seja no quesito capacitação seja no quesito conscientização.

Apesar disso, o que se observou é que os investimentos nessa área continuam a ser incipientes. Aparentemente, há uma demasiada confiança na tecnologia, como se esta fosse capaz de resolver todos os problemas de segurança. Por essa razão, há, consequentemente, um relaxamento em se identificar as fragilidades a que as pessoas estão sujeitas e, por isso mesmo, elas são os alvos preferidos daqueles que querem roubar informações. A engenharia social aparece como uma das modalidades de ataque que vem sendo maciçamente aplicada, principalmente, quando se quer roubar informações de alto valor. Nesse caso, fazem de vítimas até os usuários mais experientes.

Porém, a abordagem da sensibilização e da conscientização do usuário, tem sido criticada por alguns autores, tais como Aytes e Connolly (2003) e Siponen (2000), devido à falta de uma teoria sólida, comprovada, que possa ser aplicada e que tenha um guia de testes concretos para garantir o comprometimento dos usuários no cumprimento do seu papel na segurança da informação.

A seguir, são listados alguns autores e suas abordagens sobre a importância do fator humano para a segurança da informação.

Aytes e Connolly (2003) apresentam um modelo de comportamento do usuário, que enfatiza os fatores relativos à sua percepção, ao risco e, consequentemente, à sua escolha com base nessa percepção. Segundo esse modelo, as fontes de informação do usuário, tais como: treinamento, mídia, colegas de

trabalho, amigos, políticas, procedimentos e experiência pessoal, fornecem elementos que formam o seu conhecimento sobre ameaças e vulnerabilidades, consciência da necessidade de medidas preventivas, análise de consequências potenciais para si e para outros, das escolhas feitas e ainda, sobre os custos de um comportamento seguro. Essas informações devem ser percebidas pelo usuário, para que possam ser relevantes no momento da tomada de decisão em uma situação específica.

Assim, a percepção do usuário sobre a disponibilidade e a usabilidade de práticas seguras; a probabilidade de consequências negativas; o significado para ele, de consequências negativas; a facilidade de recuperação em caso de perda e a expectativa a respeito do comportamento dos colegas representam um fator importante no processo da escolha do comportamento que definirá a atitude a ser adotada. Os resultados, positivos ou negativos, do comportamento adotado são retroalimentados como uma fonte de informação nova.

Banerjee, Cronan e Jones (1998) buscaram identificar as características situacionais que exercem impacto na intenção de comportamento relacionado à ética dos trabalhadores da segurança da informação, quando eles são confrontados com dilemas éticos. Os resultados do estudo indicaram que a intenção do empregado de segurança da informação de adotar comportamento ético ou antiético está fortemente relacionada com o contexto da percepção individual do ambiente organizacional em que está inserido e, também, por ser influenciado por essa obrigação moral individual de realizar determinadas ações. Consequentemente, o estudo propõe que as empresas estabeleçam, claramente, seus valores éticos e os comuniquem aos seus empregados, visando garantir que as restrições comportamentais sejam observadas (BANERJEE, 1998).

Beatson (1991) discute como evitar falhas de segurança. Com esse propósito, o estudo dele sugere a adoção do princípio de privilégio mínimo possível, a análise do perfil psicológico do potencial dos novos empregados, a divisão de responsabilidades, regras claras de classificação de dados e a execução forçada da

política de segurança, através da criação e da manutenção de um alto nível de conscientização em segurança da informação. Isso se consegue através da formação adequada dos trabalhadores.

Bray (2002) afirma que as empresas são especialmente vulneráveis a falhas de segurança quando ocorrem mudanças significativas, tais como uma redução na força de trabalho. Como um meio para evitar falhas de segurança durante as mudanças organizacionais, o estudo sugere um programa de treinamento e de conscientização em segurança da informação, que aborde a engenharia social, a relação com a imprensa, a proteção de senhas; que, incentive os administradores a serem vigilantes em relação aos sistemas de avaliação e aos *logs* de segurança; que, combine com o aumento do alerta no quesito segurança física.

Cox, Connolly e Curral (2001) argumentam que o comportamento do usuário é fundamental para a segurança da informação. Por essa razão, o estudo examinou três abordagens que podem ter um impacto no comportamento dos usuários de sistemas de informação em um ambiente acadêmico: (1) uma sessão de discussão, (2) uma lista de verificação, e (3) um tutorial baseado na web. Os resultados do estudo apontam que as três abordagens parecem ser válidas para o crescimento da conscientização sobre a segurança da informação dos usuários em geral.

Forcht, Pierson e Bauman (1988) discutem a importância da consciência ética para a segurança da informação e enfatizam o papel das pessoas, as suas atitudes, as suas ações e o senso delas de certo e de errado, na abordagem de questões de segurança. O estudo propõe que a construção de uma base forte em termos de consciência ética e a reiteração constante da necessidade de se manter essa base, podem aumentar a segurança das informações em uma organização. O estudo recomenda a adoção de programas de conscientização sobre segurança da informação como um meio potencial para alcançar o resultado.

A norma brasileira NBR ISO/IEC 27002 que trata de *Tecnologia da Informação – Código de Prática para a Gestão de Segurança da Informação*, no seu

item 8.2.2. - *Conscientização, Educação e Treinamento em Segurança da Informação – Controle* (ASSOCIAÇÃO, NBR ISO/IEC 27002, 2005), consta que:

> Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriado em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções.

A norma recomenda que o treinamento de conscientização deve começar com um processo formal concebido para introduzir as políticas e as expectativas de segurança da informação da organização, antes que seja dado o acesso às informações ou aos serviços. Esses treinamentos devem incluir requisitos de segurança da informação, responsabilidades legais, bem como treinamento do uso correto dos recursos de processamento da informação, como, por exemplo, procedimentos de *logon*, o uso de pacotes de *software* e informações sobre o processo disciplinar.

Martins e Eloff (2002) apresentam um modelo para implementar e reforçar a cultura em segurança da informação, centrado em três níveis de comportamento organizacional, a saber: nível organizacional, nível de grupo e nível individual. Sugerem que a cultura de uma organização em segurança da informação deve ser melhorada, tendo em conta o comportamento humano. Os autores recomendam que cada empregado deve ser informado, através de treinamentos de conscientização, para agir de acordo com o que se espera dele, a fim de proteger os ativos de informação.

Murray (1991) descreve alguns dos problemas associados à segurança da informação. Ele argumenta que os maiores problemas de segurança são resultantes da incompetência de empregados que não entendem os perigos inerentes às suas ações. O autor enfatiza a necessidade de um programa organizacional de sensibilização em segurança da informação para superar esse problema. Assim, esse tipo de programa deve ser uma combinação de cursos, seminários, vídeos, apostilas, diretivas, lembretes e boletins informativos. Além disso,

o apoio da administração e o seu comprometimento com o programa é vital para a eficácia prática deste.

Parker (1998, 1999) propõe que a principal motivação para a segurança da informação deve vir de recompensas e de penalidades diretamente associadas ao desempenho no trabalho. Ele também afirma que os conflitos entre o desempenho no trabalho e as restrições de segurança devem ser removidos, fazendo a segurança de uma parte do desempenho no trabalho. Além disso, o autor apresenta seis fatores para uma boa segurança da informação: (1) apoio da alta administração; (2) apoio dos recursos humanos; (3) descrições de trabalho, que incluem tarefas específicas para a proteção e estabeleçam a responsabilidade por informações e por sistemas; (4) avaliações e discussões de suporte a empregados para a prática de segurança da informação nas avaliações anuais de desempenho do trabalho; (5) documentar e difundir os esforços de segurança e as recompensas concedidas; e, (6) motivar os gestores a assegurarem o seu apoio nas questões de segurança da informação.

Siponen (2000) argumenta que os programas de sensibilização para a segurança da informação devem ser fundamentados em teorias comportamentais, a fim de prover os usuários de respostas a perguntas do tipo *por que é necessário seguir as diretrizes de segurança?*. O objetivo de tais programas deve ser o de alcançar uma situação em que os usuários internalizem e sigam as políticas de segurança. A esse respeito, o autor apresenta um quadro de abordagens persuasivas, baseadas na moral, na ética, no bem-estar, na sensação de segurança, na racionalidade, na lógica e nas emoções.

Thomson e Von Solms (1997) propõem um programa de conscientização organizacional sobre segurança da informação, o qual visa conscientizar todos os usuários e as partes responsáveis pela informação sobre o valor e a importância da segurança da informação. Além disso, o programa visa sensibilizar os usuários sobre os procedimentos de segurança que devem ser seguidos por eles. Os autores identificaram três diferentes grupos-alvo para um

programa desse tipo: a alta administração, os gestores de sistemas de informação e os usuários finais. Assim sendo, propuseram os seguintes meios para implementar o programa: apresentações, *workshops*, distribuição permanente de materiais, tais como: folhetos, boletins informativos, pacotes de multimídia, lembretes, via *e-mail*, e protetores de tela.

Thomson e Von Solms (1998) defendem a importância de os empregados estarem devidamente treinados e conscientizados sobre as questões de segurança da informação, a fim de proteger os ativos de informação da organização. Eles propõem uma variedade de princípios extraídos da psicologia social (aprendizagem operante, modelagem, aprendizagem social, conformismo, obediência, reciprocidade, compromisso, atribuição, autopersuasão, dissonância, exposição, atenção, aceitação, formação, aprendizagem instrumental e retenção) a serem implantados, visando melhorar a eficiência prática no treinamento de conscientização sobre segurança da informação.

O documento *White House: The National Strategy to Secure Cyberspace, Priority III: A National Cyberspace Security Awareness and Training Program (THE WHITE HOUSE, 2003b)* descreve um programa desenvolvido pelo governo dos Estados Unidos da América, para promover um programa de conscientização nacional sobre segurança da informação. Além disso, esse programa visa garantir o treinamento em segurança e a educação necessários para a proteção da infraestrutura nacional de tecnologia da informação. Os componentes do programa são: (1) conscientização dos usuários domésticos, pequenas empresas, grandes empresas, instituições de ensino superior, setores privados, governos estadual e local; (2) auxílio na formação e na educação adequada e no aumento da eficiência dos programas federais de formação existentes; e, (3) promover suporte ao setor privado para as boas iniciativas e para as certificações profissionais amplamente reconhecidas.

Além disso, o documento *White House: The National Strategy to Secure Cyberspace, Appendix: Actions and Recommendations (A/R) Summary (THE*

WHITE HOUSE, 2003a) contempla diversas ações e recomendações que podem ser adotadas a respeito do programa nacional de treinamento e de conscientização em segurança da informação. Essas ações incluem, campanhas de conscientização, segurança de redes, programas federais de formação de profissionais em segurança da informação e desenvolvimento de programas de certificação em segurança.

Wood (2002) argumenta que, em muitos casos, as ações humanas desfazem as medidas técnicas de segurança. Consequentemente, as organizações devem se esforçar para educar os usuários e avaliar se eles estão em conformidade com as políticas da organização sobre segurança e instruí-los sobre as bases existentes. Para melhorar esses esforços, o autor descreve uma campanha de educação em segurança, chamada *Human Firewall*[13], que é um esforço internacional para ajudar os gerentes e os empregados das organizações a mudarem suas atitudes e seus comportamentos, visando melhorar a proteção dos ativos críticos de informação.

Como se viu anteriormente, muitos autores têm percebido a importância do fator humano na proteção das informações. O autor deste trabalho, por entender essa importância, incluiu o pilar *pessoas* como fundamental para o equilíbrio da segurança da informação, ao dar a ele o mesmo destaque dado a *tecnologia* e a *processos*. Afirma-se sempre que o fator humano é o elo mais fraco da corrente e, que o maior obstáculo ao processo de segurança é o próprio indivíduo. Portanto, deve-se dar a ele destaque compatível com a sua importância e, criar programas de conscientização e, também, de treinamentos.

Porém, nem sempre o vazamento de informações vem de pessoas mal treinadas ou por falta de conscientização. Muitas vezes, as informações são roubadas por pessoas que trabalham oficialmente na organização e estão legalmente autorizadas a acessá-las. Por isso, há a necessidade de se utilizar termos de

[13] *firewall* é o nome das portas antichamas usadas nas escadarias de prédios. No mundo da computação é um dispositivo que fica entre um *link* de comunicação e um computador, verificando e filtrando todo o fluxo de dados, conforme a política de segurança estabelecida. Funciona como uma barreira de proteção.

confidencialidade e de processo disciplinar, para os casos de uso indevido de informações. Esses termos permitem responsabilizar judicialmente as pessoas que causarem dano à empresa, por vazamento indevido de informações.

Portanto, ao se estabelecer um programa de segurança da informação, o fator humano deve ser considerado em todos os seus aspectos, levando-se em consideração a sua complexidade.

Cada um dos pilares tem a sua importância específica, porém como eles são interdependentes é necessário que se tenha uma visão integrada sobre eles. A segurança da informação não pode ser suportada isoladamente por um pilar, por mais importante que seja esse pilar, mas solidariamente pelos três. Como concluiu a pesquisa da Ernst & Young (2006) sobre segurança da informação, esses pilares são fundamentais para a proteção da informação, razão pela qual devem ser cuidadosamente balanceados de acordo com a relevância de cada um, na proporção do valor da informação. Assim sendo, algo estará balanceado somente quando os seus componentes ou as partes que o compõem forem contemplados em proporções adequadas e satisfatórias. Se se tiver esse cuidado os pilares poderão subsidiar ações de melhoria da segurança da informação.

4.2.5 Modelo de avaliação da segurança da informação

Não foram encontrados autores que abordam a mensuração dos três pilares que sustentam a segurança da informação, porém alguns trazem sugestões sobre o assunto.

Hagen (2008) propõe uma metodologia para medir o índice de implementação de medidas organizacionais de segurança de informações e a eficácia das medidas implementadas. Segundo o autor, essa eficácia pode ser vista a partir de quatro perspectivas inter-relacionadas:

- perspectiva da gestão de risco: medidas de segurança da informação devem reduzir o risco de incidentes indesejáveis;

- perspectiva econômica: medidas de segurança da informação devem dar retorno positivo nos investimentos;

- perspectiva legal: medidas de segurança da informação devem evitar a violação de requisitos legais; e,
- perspectiva cultural: medidas de segurança da informação devem criar uma boa cultura de segurança.

Esse autor classificou as medidas organizacionais em segurança da informação em quatro grupos e os dividiu em itens:

- Política de segurança: implementação de política de segurança da informação - item único;

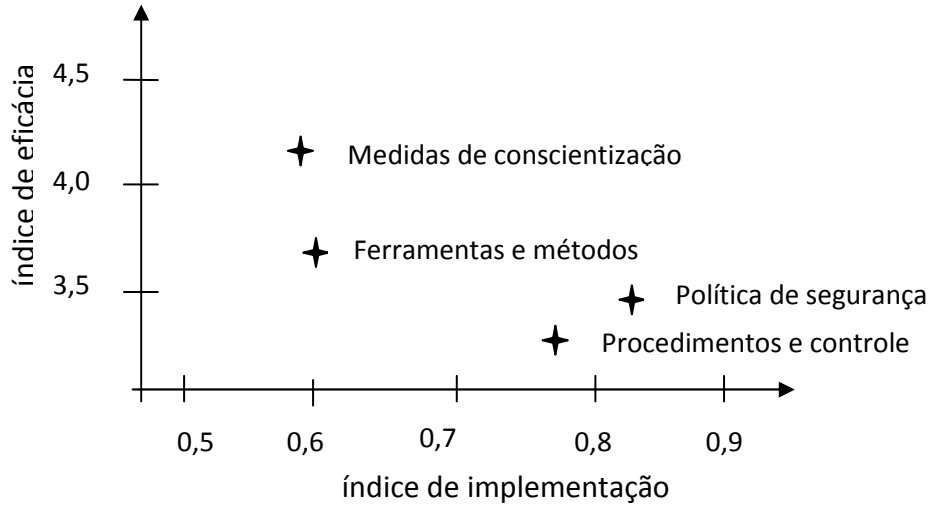
- Procedimentos e controles: composto por quatro itens - rotinas de segurança para o pessoal contratado, instruções de utilização, acordos de confidencialidade e processos disciplinares;

- Ferramentas e métodos: composto por sete itens - classificação de ativos, análise de riscos, auditoria interna, auditoria externa, KPIs (indicadores chave de desempenho), sistemas de notificação, e, planos de tratamento de incidentes;

- Criação de sensibilização: composta por cinco itens - formação/educação, campanhas de sensibilização, participação do usuário, envolvimento da alta gerência, envolvimento de todas as partes da organização em processos de aprendizagem a partir de incidentes.

O autor aplicou a metodologia em várias empresas norueguesas e analisou a resposta de 87 gerentes de segurança de organizações. O resultado está representado no gráfico 9.

Gráfico 9 – Índice de implementação de medidas de segurança *versus* índice da eficácia das medidas implementadas

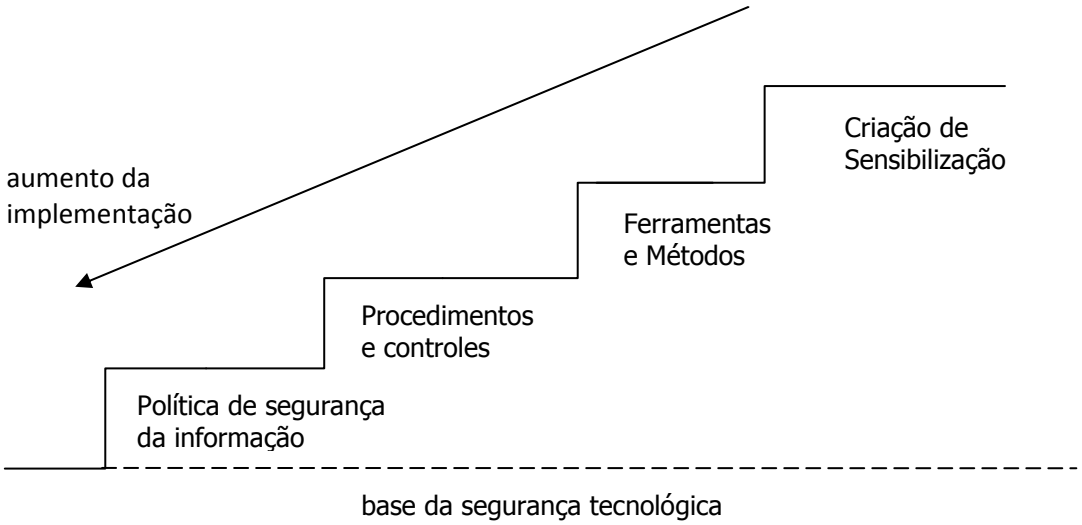


Fonte: Adaptado de Hagen, 2008.

Há, portanto, uma relação inversa entre o índice de implementação das medidas organizacionais de segurança da informação e o índice de eficácia das medidas implementadas.

A partir da análise do gráfico 9, o autor sugeriu que esses quatro grupos formem uma escada, em que o degrau mais baixo seja o que apresenta o maior índice de implementação, embora seja o de menor eficácia para a segurança da informação; e que o degrau mais alto seja o inverso, conforme figura 3.

Figura 3 - Escada de segurança da informação organizacional



Fonte: Adaptado de Hagen, 2008

O modelo, proposto por Saleh (2007) investiga o quanto a gestão da segurança da informação em uma organização está aderente à norma ISO 17799-2005. Para tanto, o autor subdivide a análise em cinco domínios (STOPE): *Strategy; Technology; Organization; People; and Environment* (estratégia, tecnologia, organização, pessoas e ambiente). Cada um desses domínios é dividido em cinco níveis, aos quais se atribui uma nota que varia entre zero e cinco, para cada domínio. Quanto mais próximo de cinco, mais aquele domínio está aderente à norma.

Menezes (2008) também propõe um modelo de avaliação da segurança da informação, centrado no usuário. Esse modelo tem por objetivo oferecer subsídios às instituições para selecionar e para analisar os indicadores de desempenho que avaliam o nível de cumprimento das diretrizes de segurança da informação, por parte dos indivíduos pertencentes àquela instituição. O modelo está dividido em três fases: estruturação; modelagem e avaliação. Na fase de estruturação, identificam-se os *stakeholders*. Na fase de modelagem, o foco principal é a escolha dos indicadores e das escalas de análise e, na fase de avaliação, faz-se a coleta de dados, calculam-se os indicadores, analisam-se os resultados, para determinar as ações corretivas em busca da melhoria de desempenho.

Patel (2008) propôs um método para avaliar a vulnerabilidade das organizações quanto às violações em questões de segurança da informação. Apesar de se terem feito muitas pesquisas sobre abordagens qualitativas, a literatura sobre métodos numéricos para quantificar riscos à segurança da informação tem sido escassa. Esse trabalho sugeriu um método para quantificar o risco em termos de valor numérico ou grau de segurança cibernética. Para ajudar a medir quantitativamente o nível de segurança cibernética de um sistema de informação baseado em computador, o autor apresentou dois índices: o índice de impacto da ameaça, que representa o risco de perda financeira; e o índice de cyber-vulnerabilidade, que representa as vulnerabilidades do sistema, baseadas em árvores de vulnerabilidade. Ao calcularem e ao compararem os índices para várias possibilidades de melhorias de segurança, os gestores podem selecionar a melhor

opção de melhoria, priorizar as escolhas pela sua eficácia relativa, e estatisticamente justificar os recursos gastos com a opção selecionada. O método, ao qualificar a segurança da informação quantitativamente, também pode ajudar os gestores a estabelecerem uma meta específica de nível de segurança que possa ser acompanhada.

A metodologia consiste de um sistema de supervisão, controle e aquisição de dados - *SCADA – Supervisory, Control and Data Acquisition*, que é subdividido em seis passos:

- Passo 1: construção da árvore de vulnerabilidades;
- Passo 2: construção da tabela de análise de danos e cálculo dos índices de impacto das ameaças;
- Passo 3: Inclusão dos valores dos índices de impacto das ameaças na árvore de vulnerabilidades;
- Passo 4: Cálculo dos valores dos índices de cyber-vulnerabilidade;
- Passo 5: Inclusão dos índices de cyber-vulnerabilidade para completar a árvore de vulnerabilidades;
- Passo 6: Repetição dos passos de dois a cinco para as melhorias de segurança propostas.

Essa metodologia foi testada mediante o uso de dados da Universidade de Louisville, Kentucky – USA (PATEL *at al.*, 2008), como um estudo de caso. O sistema *SCADA* foi implementado e, em seguida, foram comparados os índices propostos nesse sistema de informação, antes e depois de dois aperfeiçoamentos de segurança sugeridos. Assim, pôde-se identificar as vulnerabilidades de maior impacto financeiro e as maiores vulnerabilidades do sistema. Isso permitiu indicar onde se deveria investir para mitigar as fragilidades de segurança da informação.

O método *OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation*, proposto por Christopher Alberts, Audrey Dorofee, James Stevens e Carol Woody da *Carnegie Mellon University – USA*, é uma técnica de

planejamento e de estimativa estratégica de segurança, baseada em risco, que tem como alvo o risco organizacional. Essa técnica concentra-se na estratégia e em questões práticas e não somente em riscos tecnológicos e em questões táticas. Quando aplicado, o OCTAVE proporciona o nivelamento de três pontos-chave: risco operacional, práticas de segurança e tecnologia (ALBERTS, 2003). Os aspectos organizacionais, tecnológicos e operacionais da avaliação de riscos de segurança da informação são realizados pelo OCTAVE em três fases:

- Fase 1: Construção de perfis de ameaças baseados em ativos: visão organizacional para se definir os ativos críticos ao negócio e os seus requisitos de segurança.
- Fase 2: Identificação de vulnerabilidades na infraestrutura: visão tecnológica - avaliação da infraestrutura de Tecnologia da Informação e Comunicação – TIC e das suas condições em relação aos requisitos de segurança definidos.
- Fase 3: Desenvolvimento de planos e de estratégias de segurança: identificação de riscos aos ativos críticos e a criação de estratégias de proteção e de planos de mitigação de riscos.

Todos esses modelos, cada um à sua maneira, tratam da questão e ajudam na gestão da segurança da informação. Porém, nenhum deles aborda a segurança da informação sob o ponto de vista dos três pilares e da necessidade de que esses três pilares estejam balanceados.

4.3 Conclusão da revisão de literatura

O reconhecimento da importância de se protegerem as informações tem sido crescente nas organizações. O volume de ocorrências de roubo de informações, de fraudes, de invasão a *sites* e de outras formas de violação tem atingido patamares preocupantes, por gerar não somente altos prejuízos financeiros às organizações, como também problemas de imagem. Os problemas de imagem, às vezes, são mais impactantes do que o próprio prejuízo financeiro.

Assim, como reflexo dessa situação, muitas empresas estão reagindo, a fim de buscar alternativas para proteger as suas informações. Para tanto, estão destinando um volume maior de recursos para tratar das questões de segurança. Por outro lado, as fraudes se tornam cada dia mais sofisticadas e os fraudadores mais audaciosos. Na área bancária, por exemplo, tem-se constatado claramente a migração da forma de roubo de dinheiro. Assaltos a agências bancárias por bandidos com alto poder de fogo, que fazem reféns, têm diminuído, devido ao risco inerente a essa forma de abordagem e dado lugar ao roubo de senhas e à clonagem de cartões, por representarem menor risco ao delinquente. Ou seja, o roubo é mais sofisticado, por precisar de se ter maior conhecimento tecnológico e de utilizar-se, muitas vezes, de engenharia social, na qual a audácia não tem limites.

Os órgãos reguladores têm contribuído para minimizar a ocorrência de fraudes, por meio de normas mais rígidas, que exigem que as empresas adotem procedimentos mais eficazes na proteção de suas informações. Por exemplo, a Resolução 3380 do Banco Central do Brasil (BANCO, 2006), incluiu esse assunto no rol das atividades que podem trazer risco operacional às instituições financeiras. Se a instituição não regulamentar, não implantar e nem testar os procedimentos adequados de segurança da informação, deverá reservar e depositar, no Banco Central do Brasil (BACEN), um determinado valor monetário. Esse valor é calculado com base em metodologia estabelecida pelo BACEN, que indica quão preparada a instituição está para responder ao risco operacional a que está sujeita. O princípio é o mesmo utilizado já há bastante tempo, para o cálculo do risco de crédito, quando o banco tem que reservar uma importância para cobrir possíveis inadimplências dos tomadores de crédito.

Com esse mesmo intuito, regulamentações[14] do governo norte-americano vêm forçando as empresas a levar a segurança mais a sério, no sentido de exigir a proteção dos dados contra uso indevido, exposição e acesso não

[14] Lei Americana de Responsabilidade e Portabilidade dos Seguros-Saúde (HIPAA) (ESTADOS UNIDOS, 1996)
Lei Gramm-Leach-Bliley (GLBA) (WELLS, 1999)
Lei Sarbanes-Oxley (SOX) (THE SARBANES-OXLEY, 2013)

autorizado. Dessa forma, as empresas enfrentam novas obrigações legais no que diz respeito à retenção de documentos e ao gerenciamento de registros eletrônicos (LAUDON e LAUDON, 2007).

Outros órgãos normativos têm editado normas que contribuem para a melhoria da segurança das informações, como, por exemplo:

- ISO 9001:2008 – *Quality Management Systems – Requirements*: Essa norma contribui para se estabelecer um modelo de gestão da qualidade para as organizações em geral, notadamente, na padronização dos seus processos-chave. Além disso, contribui para os processos de segurança da informação, uma vez que possibilita a implementação e a manutenção dos registros adequados e necessários para garantir a rastreabilidade do processo. Contribui, ainda, para a inspeção de qualidade para os meios apropriados de ações corretivas, quando necessário (ASSOCIAÇÃO, 2008).

- NBR ISO/IEC 12207:1998 – *Tecnologia de Informação – Processos de Ciclo de Vida de Software* – ABNT, 1998: Essa norma contribui para se estabelecer um alto padrão para o desenvolvimento e para a manutenção de *softwares*. Nesse sentido, os aspectos da segurança da informação devem contemplar todo o ciclo de vida do *software* (ASSOCIAÇÃO, 1998).

- ISO/IEC 20000-1:2005 – *Information Technology – Service Management* – Parte 1: Essa norma define as melhores práticas de gerenciamento da qualidade dos serviços de TI. Os processos que fazem parte do escopo dessa norma, quando executados de acordo com o que ela estabelece, contribuem para identificar, para controlar e para mitigar as fragilidades da segurança da informação (ASSOCIAÇÃO, 2005).

- NBR ISO/IEC 27001:2006 – *Tecnologia da Informação: Técnicas de segurança - Sistema de Gestão da Segurança da Informação – Requisitos* – ABNT, 2006: Essa norma foi elaborada para prover um modelo para: estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gestão de segurança da informação - SGSI (ASSOCIAÇÃO, 2006).

- NBR ISO/IEC 27002:2005 – *Tecnologia da Informação: Código e Prática para a Gestão da Segurança da Informação* – ABNT, 2005: É um código e uma prática para a gestão de segurança da informação. Essa norma está dividida em 11 seções, cujos aspectos devem estar espalhados por vários setores de uma organização (ASSOCIAÇÃO, 2005).

Existem ainda proposições de boas práticas de governança de TI que reservam capítulos destinados à proteção de informações, como o COBIT e o ITIL. Tais proposições, quando implementadas, contribuem para a melhoria da segurança da informação.

O COBIT (*Control Objectives for Information and Related Technology*) está dividido em quatro domínios (Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar, Monitorar e Avaliar). Cada domínio está subdividido em processos e cada processo tem seus objetivos de controle. O domínio *entregar* e *suportar* trata dos processos de entrega dos serviços requeridos, principalmente, quanto aos aspectos de segurança, de treinamento e de suporte. Dois desses processos: *assegurar a continuidade dos serviços* e *assegurar a segurança dos serviços*, tratam diretamente de assuntos que contribuem para a garantia da segurança da informação (IT GOVERNANCE INSTITUTE, 2007).

O ITIL (*Information Technology Infrastructure Library*) é um conjunto de boas práticas que devem ser aplicadas na infraestrutura, na operação e na manutenção de serviços de tecnologia da informação, com o objetivo de promover a gestão, com foco no cliente e na qualidade desses serviços. Segundo

> o ITIL, os serviços de TI devem estar alinhados às necessidades do negócio e sustentar os processos da atividade fim da empresa. Dos processos detalhados pelo ITIL, há, pelo menos, quatro (gestão da continuidade dos serviços de TI, gestão da disponibilidade, gestão de incidentes e gestão de problemas) que tratam de assuntos diretamente relacionados à segurança da informação, visando melhorar a disponibilidade, a confidencialidade e a integridade das informações (REINO UNIDO, 2011).
>
> De maneira geral, todas as normas, os regulamentos, e as recomendações, apontam na direção de que toda e qualquer organização deveria conhecer os riscos de segurança a que está sujeita e, a partir daí, deveria definir ações preventivas para mitigar esses riscos. Além disso, algumas organizações deveriam, ainda, reservar uma importância monetária para cobrir possíveis ocorrências de incidentes, que as ações preventivas não foram capazes de evitar.

O diagnóstico sobre a quais riscos uma organização está sujeita, a identificação das fragilidades, o cálculo da probabilidade de ocorrência desses riscos, o impacto, a definição de quais medidas de segurança devem ser adotadas e a avaliação da eficácia dessas medidas têm sido objeto de estudo de algumas áreas, sob as mais variadas formas de abordagem. Esse fato tem gerado diferentes alternativas de intervenção.

Provavelmente, a área que mais tem estudado esse assunto seja a ciência da computação. Certamente, porque muitos ainda entendem que segurança da informação é um problema que a tecnologia tem que resolver. Porém, esse ponto de vista está sendo superado, mediante a constatação de que a tecnologia é incapaz de dar todas as respostas a essa complexa questão. Por ser esse um problema que afeta vários segmentos, o estudo da sua solução ganhará mais força e avançará mais quando diferentes ciências se associarem para debaterem sobre esse assunto.

A ciência da informação é uma área que possui estreita relação com a segurança da informação, por isso pode contribuir para o estudo e para o entendimento das questões que envolvem a necessidade de proteção da informação.

Pode, também, contribuir para a proposição de alternativas que minimizem os efeitos indesejáveis da quebra da segurança da informação. Além da interdisciplinaridade comum a ambas as áreas, a segurança da informação pode ser entendida como uma disciplina de suporte à ciência da informação, uma vez que dispõe de meios para garantir a preservação das características originais da informação para uso futuro, e é fundamental em todo o ciclo de vida da informação.

Várias áreas estão estudando a questão da segurança da informação, porém cada uma tem se dedicado mais especificamente aos aspectos que lhe afetam, e não de forma abrangente. Por exemplo, a ciência da computação tem se preocupado muito com a questão tecnológica; a administração com a questão dos processos; a psicologia e outras ciências com o comportamento humano. No entanto, há carência de áreas que realizem estudos sistemáticos que envolvam e integrem todas as demais áreas. Nesse sentido, a ciência da informação poderia contribuir com a proposição de estudos mais holísticos e interdisciplinares de segurança da informação, o que já é próprio do *corpus* de estudo da informação.

Outra abordagem importante refere-se ao valor da informação. Quando se fala em segurança, fala-se em proteger algo que tem algum valor. Não é lógico que se gastem recursos ou tempo para se proteger algo que não tenha nenhum valor. Esse raciocínio também se aplica à informação, ou seja, só se deve proteger a informação que tem algum valor. O problema está em como se determinar o valor de uma informação. Este trabalho, mesmo após extensa pesquisa, não encontrou nenhuma técnica consolidada capaz de calcular, com precisão, o valor de uma informação. Porém, encontramos algumas definições sobre valor, que contribuem para, ao menos, estabelecer comparações entre diferentes informações para que, assim, se possa saber quais informações são mais valiosas.

A primeira definição de valor, apresentada pelos economistas, registra que valor é aquilo que alguma coisa possui e que contribui para aumentar a riqueza. Visando ampliar o entendimento, Smith (1988) fez distinção entre valor de troca e valor de uso. O valor de troca está vinculado a questões monetárias: as

pessoas trocam dinheiro por produtos. Se, em determinado contexto, a informação for entendida como um produto, então, o seu valor será o quanto se está disposto a pagar monetariamente por aquela informação. Já o valor de uso refere-se não ao valor monetário da informação, mas ao desejo atendido, à utilidade, à satisfação do usuário, ao atendimento das demandas. Assim, o valor de uma informação está relacionado à potencialidade do seu uso, à sua utilidade. Ou seja, valor de uso é o benefício que uma informação traz ao seu usuário. Esse é o ponto de vista de Taylor (1986), para quem o valor da informação tem significado apenas no contexto da sua utilidade para os usuários. Dessa forma, o valor da informação não está associado internamente ao conteúdo da informação em si, mas como o usuário percebe a informação.

Há outras perspectivas sobre o valor da informação, tais como: valor de propriedade, que reflete o custo substitutivo de um bem; e, valor de restrição, que está relacionado à informação secreta ou de interesse comercial, quando o uso fica restrito apenas a algumas pessoas (CRONIN, 1990). Essa classificação refere-se à restrição de sua comunicação, e, nesses casos, é comum encontrar nas organizações a classificação da informação como ostensiva e sigilosa.

Outra forma comum de se classificarem as informações nas organizações está baseada na finalidade do seu uso. Assim, são classificadas como estratégicas, táticas e operacionais. Essa forma segue o pensamento de Chaumier (1986), que visualiza a informação com duas finalidades: para o conhecimento dos ambientes interno e externo; e para atuação nesses ambientes. Essa distinção dá uma ideia de escala de valores para as informações, o que implica diferentes níveis de proteção.

Para o gerenciamento consistente de recursos informacionais é indispensável se conhecer o valor da informação. Por isso, uma das etapas do método *Infomapping*, concebido por Burk e Horton (1988), dedica-se à determinação de custos e atribuição de valor. Para os autores, atribuir valor consiste em agregar valor às informações, o que se fundamenta na transferência de informação como

resposta intensiva a um processo humano. O enfoque desse critério está na relação entre os sistemas e os usuários, mediante o uso de cinco categorias, como a seguir: qualidade da informação em si, utilidade da informação, impacto na produtividade organizacional, impacto na eficácia organizacional e impacto na posição financeira.

Para agregar valor à informação, Taylor (1986) propôs um modelo composto de quatro processos: organização da informação; análise da informação; síntese da informação e julgamento. Uma informação que passa por esses processos se torna mais valiosa para o usuário.

Enfim, estabelecer valor à informação é uma tarefa fundamental e deve ser a primeira no processo de segurança da informação, a despeito de sua complexidade. As organizações, no processo de gestão de suas informações, devem estudar, criteriosamente, qual é a melhor forma, o melhor método para classificar e para estabelecer valor às suas informações. Sem esse passo, a proteção que se dará às informações poderá ser incompatível com o seu valor e gerar, basicamente, duas situações:

- Superproteção: nesse caso, o valor gasto com a proteção é maior do que o valor da informação, acarretando desperdício de recursos.

- Subproteção: nesse caso, a proteção é insatisfatória, por isso expõe as informações a elevados riscos. A situação mais grave é quando a organização não percebe que está enquadrada nessa condição, tendo a falsa sensação de segurança. Isso aumenta a possibilidade de trazer problemas, que podem gerar sérias consequências para a organização.

Na revisão de literatura fez-se, também, uma extensa pesquisa sobre os pilares que sustentam a segurança da informação: tecnologia, pessoas e processos.

Para a segurança da informação, a tecnologia é fundamental, principalmente na era em que vivemos, na qual a tecnologia está presente em quase todos os aspectos da vida cotidiana e, em basicamente, todas as atividades

desenvolvidas pelo homem. Grande parte das informações é gerada, armazenada, comunicada e disponibilizada via tecnologia. A tecnologia é uma forte aliada da informação, porém é igualmente perigosa quando expõe a informação a elevados riscos que ela mesma é incapaz de evitar. Por isso, não se deve usar qualquer tecnologia, nem usar a tecnologia de qualquer jeito. A escolha adequada da infraestrutura de TI deve levar em consideração os requisitos de segurança que se pretende dar à informação.

Mesmo que a tecnologia esteja totalmente apropriada, outros fatores influenciam na segurança da informação. Grande parte dos incidentes ocorre devido a alguma fragilidade encontrada nos processos. Mesmo sabendo que esse é um ponto fraco, ainda é baixo o número de organizações que mapeiam, desenham e otimizam os seus processos e que se preocupam em fazer uma análise crítica, a fim de identificar as vulnerabilidades que os processos podem abrigar.

Uma vez identificadas as fragilidades, é preciso se estabelecer e documentar formalmente quais respostas serão dadas, caso ocorra algum incidente de segurança. Quando esses procedimentos são estudados, definidos e testados proativamente, resta, no momento da crise, apenas cumprir as determinações prévias registradas nos processos. Do contrário, as soluções terão que ser desenvolvidas durante a crise, em um momento completamente desfavorável, em que a equipe técnica e os administradores estão submetidos à alta pressão e ao estresse, quase sempre gerando conflitos. Nessas condições, espera-se um resultado menos favorável do que o descrito na situação anterior.

Conhecer seus processos é um dever de toda organização. A NBR/ISO/IEC 27002:2005 (ASSOCIAÇÃO, 2005) descreve em algumas seções, com muita propriedade, a necessidade de se ter processos bem definidos, registrados, regulamentados, testados, comunicados a todos os colaboradores da organização. Esses colaboradores devem estar devidamente treinados naquilo que lhes diz respeito, para que as informações possam ser mais bem protegidas. A tecnologia

ajuda muito, mas sem processos ela se torna inócua. Portanto, tecnologia e processos devem caminhar lado a lado.

O outro pilar que compõe a tríade é pessoas. Não importa quão bem projetada seja a política de segurança da informação (PSI), ela depende de indivíduos para implementá-la. Sendo assim, o sucesso ou fracasso de uma PSI está sujeito ao comportamento do usuário frente ao rol de responsabilidades que lhe foram definidas na PSI. Esse comportamento é determinado por um conjunto amplo e complexo de fatores, o que torna esse pilar o mais frágil e também o mais difícil de ser gerido.

Por isso, as pessoas são os principais alvos dos *hackers,* quando querem roubar informações de uma organização. Utilizando-se da técnica conhecida como engenharia social os *hackers* aproximam-se das suas vítimas para tirar delas as informações que procuram. Nessa situação, não importa se o sistema foi muito bem projetado, com vários níveis de proteção, tampouco se o processo foi bem desenhado e bem implementado, porque a pessoa abordada repassa informações que ela obteve legalmente.

Portanto, um programa de conscientização deve ser o primeiro passo para a segurança da informação. Se as pessoas não estiverem devidamente conscientizadas do seu papel na segurança da informação, todo o esforço despendido com tecnologia e com processos pode ficar perdido.

Ocorre que conscientizar pessoas não é uma tarefa trivial. Pelo contrário, é de alta complexidade. Estudando essa questão, vários autores destacaram pontos que merecem a atenção dos gestores, ao lidarem com essa complexa máquina, que é o ser humano, tais como:

- modelo de comportamento rege as ações do usuário;
- fatores relativos à percepção do usuário ao risco;
- consciência ética para a segurança da informação;

- características situacionais que exercem impacto na intenção de comportamento relacionado à ética;
- cultura em segurança da informação;
- incompetência de empregados que não entendem os perigos inerentes às suas ações;
- desenvolvimento de programas de treinamento e de conscientização em segurança da informação que incluem campanhas de conscientização, segurança de redes, programas de formação de profissionais em segurança da informação e desenvolvimento de programas de certificação em segurança, dentre outros.

Ao se estudar os fatores que interferem no comportamento humano, deve-se buscar a criação de uma barreira humana, uma espécie de *human firewall*, com o objetivo de desenvolver atitudes que possam resultar em maior proteção dos ativos críticos de informação, visto que, em muitos casos, são as ações humanas que desfazem as medidas técnicas de segurança adotadas.

Dessa forma, não é só tecnologia e processos que devem andar lado a lado, mas pessoas devem ser incluídas nesse grupo, formando o tripé da segurança da informação: tecnologia, processos e pessoas. Todos esses pilares são importantes para a sustentação da segurança da informação, os quais devem estar balanceados, pois nada adianta investir apenas em um ou em dois pilares e esquecer o outro. A estrutura se romperá a partir do pilar mais frágil e a informação, que é o ativo mais importante das organizações, ficará desprotegida.

A responsabilidade social da segurança da informação não pode ser esquecida. Nesse sentido, este trabalho se enquadra na afirmação de Wersig e Nevelling (1975), segundo os quais transmitir o conhecimento para aqueles que dele necessitam é uma responsabilidade social, e essa responsabilidade social parece ser o verdadeiro fundamento da ciência da informação. Assim, parafraseando esses autores, sugerimos que proteger a informação para aqueles que dela necessitam é

uma responsabilidade social, e essa responsabilidade social parece ser o verdadeiro fundamento da segurança da informação.

A contribuição deste trabalho ocorre no campo científico, mediante a apresentação de um método alternativo para se avaliar a segurança da informação, baseado no valor da informação e nos pilares tecnologia, pessoas e processos. O uso do método poderá contribuir também para desenvolver o campo prático e auxiliar na diminuição da lacuna existente entre a intenção de proteger e o resultado efetivo da proteção. Isso porque, a estimativa do valor da informação e a identificação das fragilidades existentes nos pilares tecnologia, pessoas e processo, fornecem subsídios para que ações de correção sejam implementadas de forma mais assertiva, a fim de melhorar a segurança da informação.

5 Pressupostos, variáveis e teses

5.1 Pressupostos

Os pressupostos lançados são os seguintes:

5.1.1 Pressuposto geral

A informação estará mais segura se os requisitos que compõem os pilares tecnologia, pessoas e processos forem compatíveis com o valor da informação e, se houver equilíbrio entre esses pilares.

5.1.2 Pressupostos específicos

1° pressuposto - O valor da informação é um subsídio importante para se definirem os requisitos de segurança da informação.

2° pressuposto - O balanceamento entre os pilares tecnologia, pessoas e processos, contribui para a melhoria da segurança da informação.

5.2 Variáveis

Para verificar a sustentabilidade dos pressupostos lançados, foram estabelecidas as seguintes variáveis:

Variável do 1° Pressuposto

Relação entre o valor da informação e os requisitos de proteção estabelecidos (teve como objetivo verificar se, ao definir os requisitos de proteção, o gestor leva em consideração o valor da informação).

Variáveis do 2° Pressuposto

Equilíbrio entre os pilares tecnologia, pessoas e processos (teve como objetivo verificar se os requisitos de proteção estavam contemplados e se os pilares estavam balanceados).

5.3 Teses

As teses propostas nesta pesquisa fundamentaram-se na análise do problema central discutido neste trabalho, apresentado na item 1.1.2., na revisão da literatura, detalhada na seção 4 e nas observações provenientes da pesquisa de campo, conforme item 7.3.2. As teses são as seguintes:

Tese I – A estimativa do valor da informação contribui significativamente para se definirem os requisitos de segurança da informação.

Tese II - A informação tende a estar mais bem protegida quando os pilares tecnologia, pessoas e processos estão em equilíbrio.

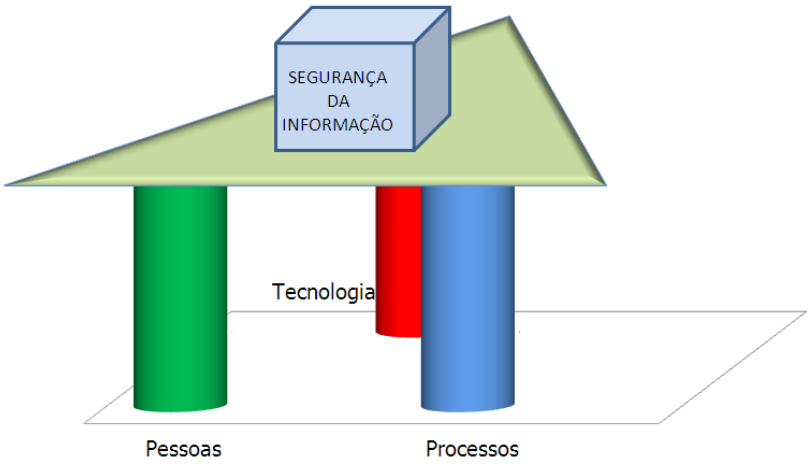
6 Proposições do estudo

6.1 Análise da segurança da informação com base no valor da informação e nos pilares tecnologia, pessoas e processos

Na geometria euclideana, encontra-se o Axioma 2 de Euclides, o qual afirma que três pontos definem um plano, desde que esses pontos não estejam alinhados. Numa visão tridimensional, representada pelos eixos "x", "y" e "z", para que um plano seja horizontal, é necessário que os três pontos que o definem, tenham a mesma ordenada "y". Quando isso não ocorre, o plano se inclina no sentido da menor ordenada "y".

Assim, com base na geometria euclideana, propõe-se uma visão da segurança da informação representada por um cubo colocado sobre um plano, que é sustentado por três pilares: tecnologia, pessoas e processos. Para que o plano esteja na horizontal, balanceado, é necessário que esses pilares tenham o mesmo tamanho (a mesma ordenada "y"). Caso contrário, o plano se inclina na direção do menor pilar, afeta a estabilidade e coloca em risco todo o esforço dedicado à segurança da informação. A figura 4 mostra essa ideia.

Figura 4 - Segurança da informação baseada nos pilares tecnologia, pessoas e processos.



Proposição do autor

A informação está dentro do cubo (segurança da informação) que a protege. Conforme se comentou anteriormente, a informação tem um valor que comparamos com o "peso" que uma estrutura tem que suportar. Quanto maior o valor da informação, mais resistente terá que ser a estrutura construída para garantir a segurança dela. Essa estrutura deve ser dimensionada com base na análise e na avaliação sistemática dos riscos a que a informação está sujeita. Conhecidos os riscos, estabelecem-se os requisitos e os respectivos controles necessários para se garantir a proteção desejada. Assim, recomenda-se estimar o valor da informação antes de se construir a estrutura que vai protegê-la. Na maioria das vezes, o que se observa é que a estrutura é construída sem se conhecer o peso (valor da informação) que terá que suportar. Como consequência, a estrutura fica mal dimensionada, e apresenta, em muitos casos, resistência inferior àquela necessária para suportar o peso (informação) que está sobre ela. Os administradores só se dão conta disso, depois que a segurança de suas informações é quebrada, expondo a organização a riscos inesperados, os quais, quase sempre, convertem-se em prejuízos, sejam monetários sejam de imagem. Portanto, o primeiro passo é estimar o valor da informação a ser protegida.

A informação, quando entendida como um produto, o seu valor pode ser estimado monetariamente. Qual o valor comercial daquela informação? Por quanto ela poderia ser vendida ou comprada? Isso ocorre, por exemplo, com empresas que trabalham com cenários. Elas buscam informações na área desejada, compilam e analisam as informações encontradas, colocam-nas no formato requerido, fazem projeções futuras do objeto em análise, e vendem-nas a interessados. Igualmente, trabalham as empresas de pesquisa de opinião, que vão para as ruas, colhem uma quantidade significativa de opiniões, tabulam os dados e os vendem a quem possa interessar. É muito comum a venda de pesquisa de opinião durante campanhas eleitorais. Essas situações se enquadram naquilo que os economistas chamam de valor de troca – o quanto o produto vale monetariamente. Troca-se produto (informação) por dinheiro.

Em alguns casos o valor da informação pode ser estimado também através da verificação de um dos objetivos de controle da segurança da informação que é a disponibilidade. Quanto tempo essa informação poderá ficar indisponível? Quanto se perde monetariamente em caso de indisponibilidade? É razoável se gastar com a proteção da informação, valores próximos ao que se poderá perder em caso de indisponibilidade dela, a fim de se evitar que essa situação ocorra.

O foco da informação pode estar voltado não para o seu valor monetário, e sim, para o desejo atendido, para a utilidade, para a satisfação do usuário, para o atendimento das demandas. Assim, o valor de uma informação poderá ser estimado pela potencialidade do seu uso e pela sua utilidade. É a teoria do valor de uso. Dessa forma, o gestor define quão relevante é a informação que lhe atende a determinadas demandas. Por exemplo, as informações colhidas em um senso do IBGE são utilizadas para se definirem determinadas políticas públicas. Quão relevantes são essas informações para atender a demandas específicas da população? É possível traçar diretrizes consistentes sem essas informações? Sabendo-se quão úteis são tais informações, pode-se definir o nível de proteção de que precisam.

Outra classificação possível para fins de proteção é quando a informação é secreta e seu uso tem que ficar restrito apenas a algumas pessoas. Muitas vezes, essa é a informação que traz a vantagem competitiva para uma empresa. A pergunta, nesse caso, é quanto se perde se essa informação se tornar pública? Aqui, pode-se enquadrar a fórmula secreta do seu produto. É o valor de restrição, quando uma informação é sigilosa e, por isso, deve ficar restrita a um grupo selecionado de pessoas.

Se não for possível estimar o valor de suas informações por nenhuma das alternativas apresentadas, classifique-as, pelo menos, como estratégicas, táticas e operacionais, pois essa é uma maneira de distinguir um grupo de outro e, assim, definir-se diferentes condições de proteção.

Estimado o valor da informação, o passo seguinte deve ser o dimensionamento dos pilares, para que venham a ter resistência compatível com o peso que deverão suportar. Ressalta-se a importância de terem o mesmo tamanho para que o plano não fique inclinado.

6.2 Metodologia de avaliação do equilíbrio entre os pilares que sustentam a segurança da informação

Avaliar o equilíbrio entre os pilares que sustentam a segurança da informação é uma tarefa complexa. O problema começa quando se tem que comparar tecnologia com processos e com pessoas. Qual é a unidade de medida que deve ser usada? Existe alguma unidade de medida comum a todos eles? Como estabelecer comparação entre coisas tão distintas?

Este trabalho propõe que cada pilar seja avaliado através da comparação de sua posição atual em relação ao seu ideal. Dessa forma, tem-se uma medida, em termos percentuais, do quão distante ele está do ideal para proteger adequadamente a informação. Cada pilar deve ser avaliado isoladamente. O resultado da avaliação se dá em termos percentuais, nos quais o ideal é que cada

um dos pilares atinja a marca de 100%. Assim, os pilares poderão ser comparados entre si, pois terão a mesma unidade de medida.

A situação ideal para cada pilar depende do valor da informação a ser protegida. A condição ideal de proteção de uma informação de baixo valor terá menos requisitos do que a condição ideal de proteção de uma informação de elevado valor.

A avaliação dos pilares deve basear-se na verificação de uma série de requisitos de controle, que compõem a situação ideal para cada pilar. Os requisitos de controle devem ser próprios para cada grupo de informações e serem estabelecidos com base no valor da informação a ser protegida e nos riscos que esta informação está sujeita.

A verificação dos requisitos ocorre de acordo com a resposta às questões específicas para cada requisito. Cada questão possui várias possibilidades de respostas. A quantidade de respostas possível a uma questão deve ser aquela que proporcione a melhor condição de capturar, com maior precisão, a opinião do entrevistado.

A escala utilizada na metodologia proposta para medir a opinião do entrevistado foi a escala de LIKERT (1932), por se adaptar melhor à forma de mensuração dos pilares aqui estudados, conforme ficou detalhado no capítulo 7 – Metodologia da pesquisa. Essa escala é usada quando se quer saber além da opinião do respondente (concordo/discordo), a intensidade dessa concordância. Para tanto, fazem-se várias afirmações que possuem diferentes níveis de concordância. Para cada nível de concordância, atribui-se um valor; e a pontuação total de um pilar é o somatório dos valores obtidos em todas as afirmações feitas sobre aquele pilar.

Cada questão ou afirmação do questionário proposto possui seis possibilidades de resposta. O valor atribuído a cada resposta consta da tabela 1:

Tabela 1 - Nível de concordância - valor

Níveis de Concordância	Valor
Concordo totalmente	6
Concordo	5
Concordo parcialmente	4
Discordo parcialmente	3
Discordo	2
Discordo totalmente	1

Entretanto, quem concorda parcialmente também discorda parcialmente. Dessa forma, para que o respondente não tenha qualquer dúvida quanto ao nível de concordância que mais represente a sua opinião, para efeito desta pesquisa, definiram-se os seguintes parâmetros de correspondência, conforme tabela 2:

Tabela 2 - Níveis de concordância – em termos percentuais

Níveis de Concordância	% de Concordância
Concordo totalmente	90 a 100%
Concordo	70 a 89%
Concordo parcialmente	50 a 69%
Discordo parcialmente	30 a 49%
Discordo	10 a 29%
Discordo totalmente	0 a 9%

Cada resposta é multiplicada por um fator de ajuste, que depende do número de perguntas respondidas e da quantidade de respostas possíveis, para que a soma total dos valores das respostas seja, no máximo, 100.

O cálculo do fator de ajuste obedece à seguinte fórmula:

$Fa = 100 / Nq \times Qr$

Onde:

Fa = Fator de ajuste;

Nq = Número de questões respondidas;

Qr = Quantidade de respostas possíveis

Portanto, para um pilar que tenha cinco questões com seis possibilidades de respostas para cada uma, o fator de ajuste será:

Fa = 100 / 5 x 6

Fa = 3,33

Segue a demonstração hipotética do tamanho de cada um dos três pilares, cujas respostas às questões formuladas foram as registradas nas tabelas 3, 4 e 5 a seguir:

Pilar pessoas

- Número de questões respondidas = 5;
- Quantidade de respostas possíveis = 6;
- Fa = 100 / 5 x 6 = 3,33

Tabela 3 – Cálculo do tamanho do pilar pessoas

Pilar Pessoas	Discordo total-mente	Discordo	Discordo parcial-mente	Concordo parcial-mente	Concordo	Concordo total-mente	Pontua-ção	Fa = 3,33	Total geral (%)
Questão 1		X					2	3,33	6,66
Questão 2			x				3	3,33	9,99
Questão 3				x			4	3,33	13,32
Questão 4	x						1	3,33	3,33
Questão 5					x		5	3,33	16,65
Total	*	*	*	*	*	*	***	***	**49,95**

Nesse exemplo, o pilar pessoas tem um tamanho de 49,95%. Ou seja, esse é o seu tamanho em relação ao que foi projetado: 100,00%.

A seguir, o cálculo hipotético dos demais pilares.

- **Pilar processos**
  - Número de questões respondidas = 6;
  - Quantidade de respostas possíveis = 6;

Fa = 100 / 6 x 6 = 2,78

Tabela 4 – Cálculo do tamanho do pilar processos

Pilar Processos	Discordo total-mente	Discordo	Discordo parcial-mente	Concordo parcial-mente	Concordo	Concordo total-mente	Pontua-ção	Fa = 2,78	Total geral (%)
Questão 1	x						1	2,78	2,78
Questão 2					x		5	2,78	13,90
Questão 3		X					2	2,78	5,56
Questão 4				x			4	2,78	11,12
Questão 5			X				3	2,78	8,34
Questão 6						X	6	2,78	16,68
Total	*	*	*	*	*	*	***	***	**58,38**

Tamanho do pilar processos = 58,38%

- **Pilar tecnologia**

  - Número de questões respondidas= 10;
  - Quantidade de respostas possíveis = 6;
  - Fa = 100 / 10 x 6 = 1,67

Tabela 5 – Cálculo do tamanho do pilar tecnologia

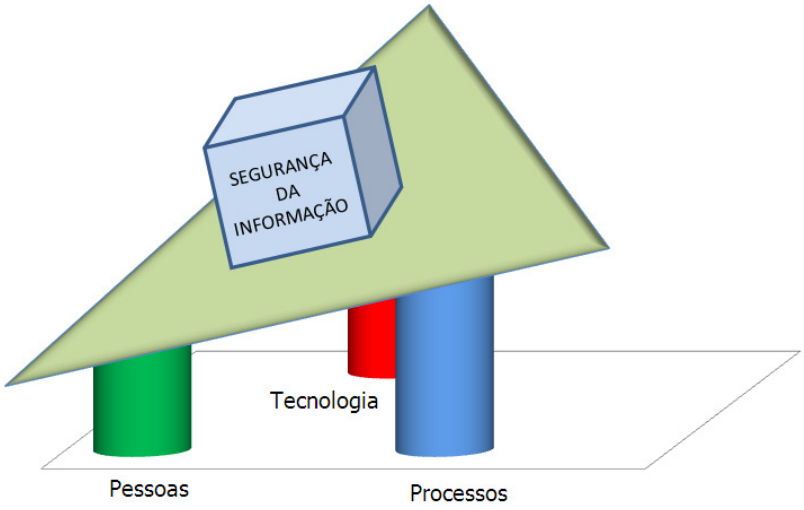
Pilar Tecnologia	Discordo total-mente	Discordo	Discordo parcial-mente	Concordo parcial-mente	Concordo	Concordo total-mente	Pontua-ção	Fa = 1,67	Total geral (%)
Questão 1	x						1	1,67	1,67
Questão 2					x		5	1,67	8,35
Questão 3		X					2	1,67	3,34
Questão 4				x			4	1,67	6,68
Questão 5			X				3	1,67	5,01
Questão 6						X	6	1,67	10,02
Questão 7		X					2	1,67	3,34
Questão 8				x			4	1,67	6,68
Questão 9					x		5	1,67	8,35
Questão 10					x		5	1,67	8,35
Total	*	*	*	*	*	*	***	***	**61,79**

Tamanho do pilar tecnologia = 61,79%

Tem-se, portanto, no exemplo dado, o seguinte balanceamento entre os pilares que sustentam a segurança da informação:

- Pessoas = 49,95%
- Processos = 58,38%
- Tecnologia = 61,79%

Figura 5 – Balanceamento dos pilares que sustentam a segurança da informação



Dessa maneira, obteve-se um diagnóstico da situação da segurança da informação, e, assim, a intervenção poderá ser mais acertada, reforçando-se os pilares. Porém, deve-se priorizar os que carecem de maior atenção, notadamente, naqueles itens cujas respostas obtiveram menor pontuação.

Essa proposição metodológica foi a utilizada na pesquisa de campo nos bancos estaduais, cujos resultados se encontram no capítulo 8 – análise dos dados e comprovação dos pressupostos.

7 Metodologia da pesquisa

Conforme afirma Saracevic (1995), os problemas de informação não podem ser abordados dentro de uma única área da atividade científica. Com isso, a

ciência da informação ainda não possui um método específico, uma metodologia que a identifica. Ao contrário, admite metodologias variadas, desde que sejam adequadas aos assuntos estudados, uma vez que os cientistas da informação não são estudiosos de áreas, e sim, de problemas.

A presente tese se enquadra nas definições de pesquisa qualitativa e a ferramenta proposta para a coleta de dados nas etapas relacionadas à pesquisa de campo foi o questionário, respondido por meio de entrevistas com os profissionais das áreas de gestão e de segurança da informação, dos bancos pesquisados.

Nesse tipo de pesquisa, um dos problemas a ser resolvido é a escolha da escala de medida a ser utilizada, de forma que possa traduzir, o mais precisamente possível, a opinião do respondente durante o processo de coleta de dados. Existem várias escalas, no entanto, foram analisadas apenas as que se seguem, por entender que eram as mais apropriadas ao objetivo desta pesquisa:

- Thurstone;
- Osgood; e
- Likert.

Começou-se com a abordagem dos seguintes tipos de escalas de mensuração:

- nominal;
- ordinal;
- razão;
- intervalar.

As escalas nominal e ordinal são escalas não métricas, isto é, as diferenças entre os números não têm nenhum significado. Os números são como rótulos, utilizados apenas para ordenar as questões. As escalas razão e intervalar são escalas métricas, ou seja, as diferenças entre os números têm significado preciso e indicam um intervalo, uma distância. A seguir, exemplificou-se cada uma delas:

- **Escalas nominais**

P. O que mais pesa na definição do seu voto a um candidato a deputado federal?

1. Sua amizade com o candidato
2. O partido de filiação do candidato
3. A proposta de trabalho do candidato
4. A honestidade do candidato

- **Escalas ordinais**

P. Quantas pessoas residem em sua casa?

1. Menos de 3
2. Entre 3 e 5
3. Entre 6 e 8
4. Mais do que 8

- **Escalas de intervalo**

Não há um zero absoluto, ou seja, o início de uma escala é diferente do início de outra escala.

P. Qual é o ponto de congelamento e de fervura da água?

Fenômeno	Escala Celsius	Escala Fahrenheit
Congelamento	0° C	32° F
Fervura	100° C	212° F

- **Escalas razão**

Há um zero absoluto, e somente a unidade de medida é arbitrária. Por exemplo, medidas de altura, de renda, de idade, etc.

Quadro 1 - Resumo dos tipos de escalas de mensuração

Escala	Característica	Uso em *marketing*	Estatísticas possíveis
nominal	Identidade, definição única de números.	Marcas, sexo, raças, cores, tipos de lojas, regiões, uso/não uso, gosta/não gosta, e a toda variável a que se possa associar números para identificação.	Moda, percentagens, teste binomial, teste Qui-quadrado, Mcnemar, Cochran Q.
ordinal	Ordem dos números.	Atitudes, preferências, opiniões, classes sociais, ocupações	Medianas, quartis, decis, percentis, teste Mann-Whitney, teste U, Kruskal Wallis, Correlação de postos.
intervalo	Comparação de intervalos.	Atitudes, opiniões, conscientização, preferências, números-índices.	Média, intervalo, amplitude total, amplitude média, desvio médio, variância, desvio padrão, teste z, teste t, análise de variância, correlação de produto-momento.
razão	Comparação de medidas absolutas, comparação de proporções.	Idade, preço, número de consumidores, volume de vendas, renda, patrimônio.	Todos os do item anterior e mais: média geométrica, média harmônica, coeficiente de variação.

Fonte: Mattar (2001)

- **ESCALA DE THURSTONE**

A escala de Thurstone e Chave (1929) é uma escala de intervalos aparentemente iguais, que pode ser usada quando não se interessa saber a intensidade do sentimento do respondente, mas apenas se ele concorda ou não com a questão posta. Exemplo:

P. O Brasil vive em plena democracia.

( ) Concordo ( ) Discordo

P. O Plano Real foi o melhor plano econômico brasileiro.

( ) Concordo ( ) Discordo

- **ESCALA DE OSGOOD**

A Escala de Osgood (1957) também é conhecida como escala do diferencial semântico. Consiste, basicamente, em uma escala bipolar de sete pontos cujos extremos são definidos por um adjetivo ou por uma frase adjetivada, como no exemplo a seguir:

- Assinale com um **X** o espaço em branco que melhor indica a sua posição.

P. O cinema brasileiro é:

profissional :__:__:__:__:__:__:__: amador

P. A justiça brasileira é:

rápida :__:__:__:__:__:__:__: lenta

A limitação dessa escala é que, muitas vezes, torna-se difícil para o pesquisador, estabelecer antônimos perfeitos para os adjetivos que deverão compor as frases a serem submetidas aos respondentes.

- **ESCALA DE LIKERT**

Proposta por Rensis Likert (1932), a escala de Likert tem semelhança com a escala de Thurstone, porém é usada quando se quer saber além da opinião do respondente (concordo/discordo) a intensidade dessa concordância. Para tanto, uma pergunta, uma afirmação ou uma frase possui várias categorias de respostas. Para cada resposta, atribui-se um número e a pontuação total daquela questão, em uma amostra de vários questionários, é o somatório das pontuações obtidas naquele item. Existem escalas de Likert, que variam de quatro a onze categorias, mas as escalas de quatro e de cinco

categorias são as mais populares. As categorias dependem do tipo de questão e da criatividade do pesquisador, como por exemplo:

P. O seu envolvimento em algum tipo de trabalho social que visa diminuir a violência é:

(0) sem nenhuma importância;
(1) pouco importante;
(2) importante;
(3) muito importante.

P. O seu envolvimento em algum tipo de trabalho social que visa diminuir a violência é:

(0) muito baixo;
(1) baixo;
(2) médio;
(3) alto;
(4) muito alto.

P. O incentivo à prática esportiva na infância e na adolescência é um excelente instrumento de combate à violência:

(0) discordo totalmente;
(1) discordo;
(2) indiferente;
(3) concordo;
(4) concordo totalmente.

Uma vantagem da escala de Likert é que ela indica a direção da atitude do respondente em relação a cada afirmação. A discussão passa a ser com relação ao número de categorias a ser definido na escala. Nesse sentido, a Teoria da Resposta ao Item - TRI se apresenta como uma alternativa para investigar o número de categorias a ser definido na escala de Likert (ANDRADE, 2000). Por outro lado, a presença da categoria central, que representa uma posição neutra ou uma indecisão, tem sido motivo de

discussão no uso dessa escala, uma vez que pode induzir o respondente a assumir essa posição sempre que ele não tiver convicção de sua resposta ou achar que é melhor não se comprometer. Incluir a opção "não sei" ou "não se aplica" no exterior da escala gradual, por exemplo, 0, 1, 2, 3, 4 e Não sei/Não se aplica, é uma ideia para evitar esse problema na construção dessa escala.

P. O incentivo à prática esportiva na infância e na adolescência é um excelente instrumento de combate à violência:

(0) discordo totalmente;
(1) discordo;
(2) indiferente;
(3) concordo;
(4) concordo totalmente
(5) não sei

Ao elaborar um questionário, o pesquisador precisa conhecer bem o assunto, para que o questionário seja abrangente e efetivo, a fim de que a pesquisa possa ser cientificamente validada. Antes de se aplicar um questionário, é conveniente que ele seja avaliado, com o objetivo de verificar se as questões formuladas comprovarão ou não os pressupostos, por meio das variáveis de pesquisa.

Considerando-se as características desta pesquisa, optou-se por utilizar a escala de Likert nos questionários utilizados para se colher a opinião dos entrevistados, por entender que essa escala se adapta com maior precisão aos objetivos deste trabalho. Optou-se, também, por não ter a categoria central, para se evitar a possibilidade da posição neutra ou da indecisão e incluiu-se a opção "não se aplica".

7.1 Delimitação do escopo do estudo

O presente trabalho foi idealizado a partir de observações sobre a quantidade significativa de empresas que têm tido problemas com a segurança de

suas informações. Apesar de estarem destinando mais recursos para as questões de segurança, os resultados obtidos continuam insatisfatórios.

A mídia noticia, a cada dia, eventos de quebra da segurança, tais como: invasões a *sites* para roubo de informações, adulteração de informações, clonagem de cartões, roubo de senhas, indisponibilidade de sistemas e de *sites.* Mais recentemente, a mídia tem noticiado ações conhecidas como guerra cibernética, que envolve não somente empresas, mas até mesmo nações.

Assim, o resultado dessas ações, invariavelmente, tem sido prejudicial aos que foram vítimas da investida contra o seu patrimônio informacional. Com base nessa realidade, este trabalho procurou examinar como o valor da informação e os pilares tecnologia, pessoas e processos podem subsidiar ações de segurança da informação.

A primeira necessidade que se constatou foi a de certificar-se se a informação tem, de fato, ocupado posição de relevância nas organizações. Do contrário, talvez se esteja dedicando tempo e esforço àquilo que não tem valor.

Durante a pesquisa foram encontrados, em abundância, autores que defendem a ideia de que a informação tem assumido um papel tão significativo, a ponto de ser considerada, para algumas organizações, o seu ativo mais importante e mais valioso. Para Drucker (1993), a informação tornou-se algo tão importante que ele prevê a troca do binômio capital/trabalho pelo binômio informação/conhecimento, como fator determinante para o sucesso empresarial. Por ser a informação algo tão relevante para a gestão das organizações, inferiu-se que era oportuno o estudo de sua segurança.

Dessa maneira, o presente trabalho tem como escopo principal o estudo da segurança da informação, que é um assunto amplo e envolve múltiplos aspectos. Assim, o foco recaiu sobre o estudo dos pilares tecnologia, pessoas e processos, devido à relevância que têm para a proteção adequada da informação.

Além disso, observou-se que a segurança requerida de uma informação é diretamente proporcional ao seu valor, ou seja, quanto maior for o valor da informação, maior deverá ser a sua proteção. Assim sendo, este trabalho teve como escopo adicional o estudo da importância do valor da informação para a definição dos requisitos de proteção dela.

De forma resumida, o escopo desta pesquisa foi a segurança da informação, com foco específico no estudo do valor da informação e dos pilares tecnologia, pessoas e processos.

Embora a motivação para este estudo tenha nascido em uma instituição financeira e a pesquisa de campo ter sido realizada, também em instituições financeiras, as aplicações das proposições aqui contidas podem ser implementadas em qualquer tipo de empresa.

7.2 Caracterização do universo e da amostra

As instituições bancárias foram visualizadas como um excelente laboratório para a pesquisa de campo, pelo fato de, talvez, ser esse um dos setores mais avançados em assuntos de segurança da informação. Isso se deve, em parte, por ser um setor fortemente regulamentado e, além disso, devido às exigências que o próprio mercado impõe ao tipo de serviço prestado.

Esta pesquisa foi realizada nos bancos estaduais brasileiros, a saber: Banco de Brasília - BRB; Banco do Estado do Rio Grande do Sul - Banrisul; Banco do Estado de Sergipe - Banese; Banco do Estado do Espírito Santo – Banestes e Banco do Estado do Pará - Banpará. Esses são os bancos estaduais existentes na atualidade, no Brasil. Portanto, a amostra abrange 100 % desse segmento. A condição imposta por essas instituições foi absolutamente razoável quanto ao compromisso de confidencialidade. O pesquisador fez um compromisso formal de não revelar, em hipótese nenhuma, as respostas aos questionários e os dados das instituições. Para cumprir essa exigência e, ao mesmo tempo, expor os dados para serem analisados nesta pesquisa, os bancos são aqui identificados simplesmente

como Banco A, Banco B, Banco C, Banco D e Banco E. Apenas o pesquisador conhece a identidade de cada um desses bancos. Essa foi a única maneira de se conseguirem os dados necessários para dar consistência às propostas formuladas nesta pesquisa.

No momento da captura dos dados, uma questão apareceu, mesmo não sendo o foco desta pesquisa, que poderá ser discutida, mais apropriadamente, na área de administração. Tratou-se do posicionamento da área de segurança da informação no organograma de uma instituição. Essa localização pode ser um indício do grau de importância que se dá às questões de segurança na instituição. O mais frequente é encontrá-la como parte da estrutura da área de tecnologia da informação. A *10ª Pesquisa Nacional de Segurança da Informação*, conduzida pela empresa Módulo (2006), constatou um progresso em relação à estruturação da área de segurança da informação. Apesar disso, constatou também que, em boa parte das empresas pesquisadas (28%), a tarefa de cuidar da segurança da informação ainda compete ao gerente de TI/Redes. Em algumas (16%), o principal responsável pela segurança da informação é o diretor de TI/CIO[15] e, somente em poucas empresas (13%), existe o cargo de CSO[16]/diretor de segurança, que é um cargo específico para gerir a segurança da informação. Isso se deve, em grande parte, ao pensamento ainda muito presente, de que segurança da informação é assunto de tecnologia.

Esse pensamento, conforme já foi largamente evidenciado neste trabalho, vem dando lugar a outro, mais amplo, de que segurança da informação é uma questão do negócio. Apesar de a tecnologia ter uma participação importantíssima nas questões de segurança, sozinha é insuficiente para solucionar todo o problema.

Dessa forma, o que se pôde constatar, foi que a segurança da informação está inserida em outras áreas que não a de tecnologia e, várias vezes,

[15] Chief Information Officer
[16] Chief Security Officer

ligada diretamente ao presidente da instituição. Isso mostra que esse problema perpassa toda a instituição e, por sua relevância, deve ser de supervisão direta do próprio presidente.

A norma brasileira NBR/ISO/IEC 27.002:2005 (ASSOCIAÇÂO, 2005) que é um código de prática para a gestão de segurança da informação, está dividida em 11 seções, cujos aspectos devem estar espalhados por vários setores de uma organização e não apenas na tecnologia.

As empresas que dão maior importância à segurança da informação estão caminhando para um desenho no qual a elaboração, a supervisão e o acompanhamento da Política de Segurança da Informação – PSI deve ficar centralizado em uma área responsável. A despeito disso, a construção da PSI deve ter a participação ativa de todas as áreas da instituição. As ações relacionadas à execução da PSI devem ser descentralizadas, isto é, cada área afetada pela PSI deve executar a parte da política que está sob sua responsabilidade.

Assim, a área de tecnologia é a responsável em executar a parte da PSI que se referir à tecnologia, notadamente, *hardware, software*, ativos de rede, controle de acesso aos sistemas, dentre outros. A área de pessoal é a responsável pela parte da PSI que se referir a pessoas, tais como: treinamento, capacitação, programas de conscientização, compromissos de confidencialidade e outros correlatos. A área de organização é a responsável pelas atividades que envolver o desenho/mapeamento de processos, bem como pela identificação de fragilidades e a proposição de novos fluxos que possam otimizar os processos e mitigar os riscos identificados. A área de serviços gerais é a responsável pelas atividades relacionadas à segurança física. A área de conformidade deve se preocupar com a observância do cumprimento das leis, das regulamentações e das normas aplicáveis.

Dessa maneira, ao se entender que segurança da informação é algo muito maior do que a própria tecnologia, deixa-se de imputar a ela a responsabilidade total pela segurança da informação, o que já será um avanço.

7.3 Etapas da pesquisa

Esta pesquisa iniciou-se com uma discussão de cunho teórico, etapa em que se fez a revisão de literatura e se estabeleceu a fundamentação teórica dos assuntos a serem estudados. Posteriormente, foram apresentadas as proposições do autor; e, finalmente, foram apresentadas a aplicação da metodologia proposta e a análise dos seus resultados.

7.3.1 Fundamentação Teórica

A etapa teórica discorreu, inicialmente, sobre o problema central, objeto principal de investigação desta pesquisa, quando se chegou ao seguinte questionamento: Como o valor da informação e os pilares tecnologia, pessoas e processos podem subsidiar ações de segurança da informação?

O passo seguinte foi a revisão de literatura, que, ao longo do desenvolvimento deste trabalho, trouxe subsídios importantes que contribuíram para melhor compreensão e melhor fundamentação do problema, bem como para as definições metodológicas adotadas. A revisão de literatura foi dividida em dois aspectos básicos:

a) contextualização do problema no âmbito da área de estudo;

b) análise do referencial teórico.

Para contextualizar o problema na área de estudo, investigou-se a existência de trabalhos sobre segurança da informação no campo da ciência da informação. Embora seja ainda discreta a quantidade de estudos existentes sobre esse assunto, alguns autores já discutem a pertinência de segurança da informação ser objeto de estudo da ciência da informação.

Uma das razões para isso é que o interesse das áreas recai sobre o mesmo objeto de estudo, que é a informação. A diferença talvez seja a especificidade da segurança da informação, cujo olhar se volta mais para a

informação que possui algum valor. Assim, parece que o objeto de estudo da segurança da informação está contido no objeto de estudo da ciência da informação, o que reforça a sugestão das questões de segurança receberem mais atenção nos domínios da ciência da informação.

Em seguida, construiu-se um referencial teórico a partir da revisão de literatura sobre os assuntos que envolveram tanto o problema quanto os objetivos do estudo, a saber: informação, valor da informação, segurança da informação, pilares que sustentam a segurança da informação e modelos de avaliação da segurança da informação.

Com base nesses levantamentos, nos estudos e nas discussões, este trabalho propôs um método de avaliação da segurança da informação, baseado no valor da informação e nos pilares tecnologia, pessoas e processos, e, além disso, apresentou uma metodologia para a mensuração desses três pilares.

Outra questão que mereceu atenção especial neste trabalho foi a verificação da coerência entre o problema, o objetivo geral, os objetivos específicos, o pressuposto geral, os pressupostos específicos, as variáveis e as teses. Dessa forma, procurou-se estabelecer o relacionamento entre esses itens, da seguinte forma:

Após discorrer sobre a problemática da segurança da informação, formulou-se a pergunta central que motivou esta pesquisa:

> Como o valor da informação e os pilares tecnologia, pessoas e processos podem subsidiar ações de segurança da informação?

Buscando identificar alternativas que contribuíssem para tornar as ações de segurança da informação mais efetivas e, assim, melhorar os seus resultados, estabeleceu-se o seguinte objetivo geral:

> Propor um método de avaliação da segurança da informação baseado no valor da informação e nos pilares tecnologia, pessoas e

processos, de modo a subsidiar ações de proteção da informação em instituições bancárias.

Com base no objetivo geral, estabeleceram-se os seguintes objetivos específicos, que são mais operacionais, mas que, juntos, contribuíram para se alcançar o objetivo geral:

1. Verificar como os gestores, em instituições bancárias, estimam o valor da informação.

2. Verificar se os gestores, em instituições bancárias, utilizam o valor da informação como subsídio para a definição dos requisitos de proteção da informação.

3. Propor uma metodologia de medição dos pilares tecnologia, pessoas e processos, de tal maneira que o possível desequilíbrio existente entre eles possa ser evidenciado.

4. Estudar a aplicabilidade da avaliação do equilíbrio dos pilares tecnologia, pessoas e processos nas ações de segurança da informação.

A partir da análise da problemática, lançou-se um pressuposto geral, visando propor, preliminarmente, alternativas para melhorar a proteção das informações que fossem compatíveis com o objetivo geral da pesquisa:

A informação estará mais segura se os requisitos que compõem os pilares tecnologia, pessoas e processos forem compatíveis com o valor da informação e, se houver equilíbrio entre esses pilares.

Como consequência do pressuposto geral, e guardada a coerência com os objetivos do trabalho, foram lançados os seguintes pressupostos específicos:

1° - O valor da informação é um subsídio importante para se definirem os requisitos de segurança da informação.

2° - O balanceamento entre os pilares tecnologia, pessoas e processos contribui para a melhoria da segurança da informação.

Com base nos pressupostos específicos, foram estabelecidas as variáveis enumeradas a seguir, que, após terem sido testadas mediante pesquisa de campo, puderam validar a consistência dos pressupostos lançados:

1. Relação entre o valor da informação e os requisitos de proteção estabelecidos (teve como objetivo verificar se, ao definir a proteção, o gestor levava em consideração o valor da informação).

2. Equilíbrio entre os pilares tecnologia, pessoas e processos (teve como objetivo verificar se os requisitos de proteção estavam contemplados e se os pilares estavam balanceados).

A partir das medições/verificações e da análise dos itens anteriores, as seguintes teses foram formuladas. Essas teses podem ser alternativas para subsidiar ações de segurança da informação, visando melhorar os resultados dessas ações, e, também, o retorno dos investimentos das empresas em segurança da informação.

Tese I – A estimativa do valor da informação contribui significativamente para se definirem os requisitos de segurança da informação.

Tese II - A informação tende a estar mais bem protegida quando os pilares tecnologia, pessoas e processos estão em equilíbrio.

O quadro 2 ilustra a relação entre os itens da pesquisa:

Quadro 2 - Relacionamento entre os itens da pesquisa

PROBLEMA	Como o valor da informação e os pilares tecnologia, pessoas e processos podem subsidiar ações de segurança da informação?			
OBJETIVO GERAL	Propor um método de avaliação da segurança da informação baseado no valor da informação e nos pilares tecnologia, pessoas e processos, de modo a subsidiar ações de proteção da informação em instituições bancárias.			
OBJETIVOS ESPECÍFIC0S	1. Verificar como os gestores, em instituições bancárias, estimam o valor da informação.	2. Verificar se os gestores, em instituições bancárias, utilizam o valor da informação como subsídio para a definição dos requisitos de sua proteção.	3. Propor uma metodologia de medição dos pilares tecnologia, pessoas e processos, de tal maneira que o possível desequilíbrio existente entre eles possa ser evidenciado.	4. Estudar a aplicabilidade da avaliação do equilíbrio dos pilares tecnologia, pessoas e processos nas ações de segurança da informação.
PRESSUPOSTO GERAL	A informação estará mais segura se os requisitos que compõem os pilares tecnologia, pessoas e processos forem compatíveis com o valor da informação e, se houver equilíbrio entre esses pilares.			
PRESSUPOSTOS ESPECÍFICOS	1. O valor da informação é um subsídio importante para se definirem os requisitos de segurança da informação.		2. O balanceamento entre os pilares tecnologia, pessoas e processos, contribui para a melhoria da segurança da informação.	
VARIÁVEIS	1. Relação entre o valor da informação e os requisitos de proteção estabelecidos (teve como objetivo verificar se ao definir os requisitos de proteção o gestor leva em consideração o valor da informação).		2. Equilíbrio entre os pilares tecnologia, pessoas e processos (teve como objetivo verificar se os requisitos de proteção estavam contemplados e se os pilares estavam balanceados)	
TESES	1. A estimativa do valor da informação contribui significativamente para se definirem os requisitos de segurança da informação.		2. A informação tende a estar mais bem protegida quando os pilares tecnologia, pessoas e processos estão em equilíbrio.	

7.3.2 Pesquisa de campo

Essa etapa foi destinada à coleta de dados para realizar as verificações/medições das variáveis. Após a tabulação e a análise dos dados captados em campo, pôde-se verificar o atingimento dos objetivos da pesquisa e propor, ainda que preliminarmente, algumas teses que ajudaram a explicar o problema estudado neste trabalho.

7.3.2.1 Instrumento de coleta de dados

Para realizar a pesquisa de campo, o primeiro passo foi definir que se utilizaria um questionário como ferramenta básica para a coleta de dados. Para tanto, escolheu-se o estruturado fechado, por ser um instrumento em que as perguntas ou as afirmações apresentam alternativas de respostas fixas e preestabelecidas. Esse tipo de questionário traz algumas vantagens, tais como: facilidade de aplicação, rapidez no ato de responder, apresenta pouca possibilidade de erro, simplicidade e objetividade no processo de análise e de comparação das respostas do grupo de entrevistados. Teve-se o cuidado de dedicar bastante tempo à preparação dele, para garantir que todas as opções de respostas fossem oferecidas, mas, principalmente, para que não se esquecesse de nenhuma questão importante para a análise do objeto de estudo.

Assim, construiu-se o questionário com base nos requisitos de segurança recomendados pelas normas da ABNT, NBR ISO/IEC 27.001 (ASSOCIAÇÃO, 2006) e NBR ISO/IEC 27.002 (ASSOCIAÇÃO, 2005), acrescidas de algumas questões que contribuíram para detalhar melhor os aspectos investigados na pesquisa.

7.3.2.2 Cotejamento dos objetivos e variáveis da pesquisa com os itens do questionário

Uma das principais tarefas durante a elaboração de um questionário é verificar sua validade e sua eficácia para se atingirem os objetivos propostos na pesquisa. Para tanto, é fundamental que o pesquisador se certifique de que as

questões constantes do questionário guardam estreita ligação com os objetivos da pesquisa. Dessa forma, as respostas ao questionário devem ser suficientes para que o pesquisador realize as medições/verificações previstas, ao lançar as variáveis.

Por ser a segurança da informação algo de grande complexidade, o ideal é que para cada fragilidade identificada exista uma ação mitigadora do risco da quebra de segurança, originada a partir daquela fragilidade. Por isso, convém que no questionário exista, pelo menos, uma questão relacionada a cada fragilidade identificada. Como este é um trabalho acadêmico e o que se pretende aqui é demonstrar a validade das questões propostas, o questionário foi reduzido, de modo que contivesse apenas os requisitos suficientes para alcançar os objetivos da pesquisa. Em uma aplicação futura desta metodologia, com vistas a diagnosticar mais profundamente a situação da segurança da informação em uma instituição, a quantidade de questões poderá ser ampliada, de acordo com o porte de cada instituição e com o valor da informação que se pretende proteger. Nesse caso, basear-se nos itens de controle previstos na NBR ISO/IEC 27.002, acrescidos dos objetivos de controle em segurança da informação propostos pelo COBIT, e nos processos previstos no ITIL, é uma alternativa consistente para se elaborar o questionário. Ao ser respondido com precisão e, se possível, acompanhado de evidências, o questionário tem a potencialidade de apresentar o *status quo* da segurança da informação muito próximo da realidade da empresa analisada.

O questionário proposto para a pesquisa de campo foi dividido em quatro partes, as quais têm os seguintes propósitos:

- **Parte I – Valor da informação** (Apêndice 1)
    - **Conteúdo e propósito**: constou de cinco questões fechadas e uma aberta, cujo objetivo foi verificar se a instituição respondente possuía uma metodologia para se estimar o valor da informação. Em caso afirmativo, se a metodologia era observada; e, se havia compatibilidade entre o valor da informação e o custo de sua proteção.

- **Relação com os objetivos e com as variáveis**: as questões propostas no questionário sobre o valor da informação foram elaboradas com o propósito de guardar relação direta com os seguintes objetivos específicos: Verificar como os gestores, em instituições bancárias, estimam o valor da informação; e, verificar se os gestores, em instituições bancárias, utilizam o valor da informação como subsídio para definirem os requisitos de proteção da informação. A variável proposta, relacionada com essa parte do questionário, foi a seguinte: Relação entre o valor da informação e os requisitos de proteção estabelecidos, cujo objetivo foi verificar se, ao definir os requisitos de proteção, o gestor levava em consideração o valor da informação.

- **Parte II – Pilar pessoas** (Apêndice 2)
  - **Conteúdo e propósito**: constou de nove questões fechadas e uma aberta, cujo objetivo foi mensurar o pilar pessoas.

- **Parte III – Pilar processos** (Apêndice 3)
  - **Conteúdo e propósito**: constou de onze questões fechadas e duas abertas, cujo objetivo foi mensurar o pilar processos.

- **Parte IV – Pilar tecnologia** (Apêndice 4)
  - **Conteúdo e propósito**: constou de quatorze questões fechadas e duas abertas, cujo objetivo foi mensurar o pilar tecnologia.

Para mensurar os pilares, utilizou-se a metodologia proposta neste trabalho, descrita na item 6.2.

- **Relação com os objetivos e com as variáveis**: as questões propostas nos questionários sobre os pilares foram elaboradas com o propósito de guardar relação direta com os seguintes objetivos específicos: Propor uma metodologia de medição dos pilares tecnologia, pessoas e processos, de tal maneira que o possível desequilíbrio existente entre eles possa ser

evidenciado; e, estudar a aplicabilidade da avaliação do equilíbrio dos pilares tecnologia, pessoas e processos nas ações de segurança da informação. A variável proposta, relacionada com essa parte do questionário, foi a seguinte: Equilíbrio entre os pilares tecnologia, pessoas e processos, cujo objetivo foi verificar se os requisitos de proteção estavam contemplados e se os pilares estavam balanceados. Com as respostas às questões propostas, percebeu-se a importância que cada instituição atribuía aos pilares; pôde-se calcular o tamanho de cada um deles e verificar como estava o balanceamento entre eles. Dessa forma, identificou-se quais eram os requisitos de segurança da informação que necessitavam de ações de reforço.

7.3.2.3 Coleta dos dados

Inicialmente, por não se saber como estava estruturada a área de segurança da informação nos bancos pesquisados, os procedimentos de pesquisa incluíram o cuidado de conhecer previamente a estrutura de segurança de cada um dos bancos, para endereçar os questionários aos respondentes corretos e, assim, captar, com a maior fidedignidade possível, a realidade das questões pesquisadas.

Dessa forma, após o contato prévio com os responsáveis pela segurança da informação de cada um dos bancos pesquisados, seguido de uma entrevista explicativa sobre o trabalho, os questionários foram enviados, via *e-mail*, os quais foram devolvidos posteriormente, devidamente preenchidos.

8 Análise dos dados e comprovação dos pressupostos

Nesta seção estão apresentados os dados coletados nos bancos pesquisados, que, após analisados, serviram de base para se verificar o atingimento dos objetivos deste trabalho, bem como, para se comprovar os pressupostos.

8.1 Valor da informação

Os objetivos deste trabalho relacionados ao valor da informação foram os seguintes: verificar como os gestores, em instituições bancárias, estimam o valor da informação; e verificar se os gestores, em instituições bancárias, utilizam o valor da informação como subsídio para definirem os requisitos de proteção da informação.

A tabela 6 mostra a consolidação dos dados obtidos com a aplicação do questionário nos bancos pesquisados no que se refere ao valor da informação.

Tabela 6 - Respostas ao questionário sobre o valor da informação

Instituição		Banco A		Banco B		Banco C		Banco D		Banco E		Média	
Item	**Questões/Afirmações**	Sim	Não	Sim	Não	Sim	Não	Sim	Não	Sim	Não	Sim	Não
	VALOR DA INFORMAÇÃO	****	****	****	****	****	****	****	****	****	****	****	****
1	O valor da informação é estimado antes de se definir a sua proteção?	X			X		X		X		X	1	4
2	Existe uma metodologia definida e estabelecida para se estimar o valor da informação a ser protegida?		X		X		X		X		X	-	5
2.1	Se sim, a metodologia existente para estimar o valor da informação se apoia em teorias, tais como: valor de uso*, valor de troca*, valor de restrição* ou outra (especificar)?		X		X		X				X	NA	NA
2.2	Se não, existe algum critério para se classificar a informação que leve em consideração questões estratégicas (informação estratégica, tática ou operacional), ou questões de sigilo (ostensivo, confidencial) ou criticidade?	X		X		X			X	X		4	1
3	Ao se definir qual a proteção que se dará à informação tem-se o cuidado de calcular o custo da proteção e compará-lo com o valor atribuído à informação, para que o custo da proteção não seja maior do que o valor da informação?	X			X		X		X		X	1	4

A resposta ao item 1 indicou a existência de relação entre o valor da informação e a proteção a ela destinada. Os resultados obtidos sujerem que quase a

totalidade os gestores dos bancos pesquisados não estimam e, portanto, desconhecem o valor da informação que está sendo protegida. Quando não se conhece o valor do ativo objeto da proteção, pode-se incorrer no risco de se atribuir um tipo de proteção incompatível com o valor do que se quer proteger. Nesse caso, é possível que os requisitos de proteção estejam muito aquém do valor do bem protegido, tornando-o altamente vulnerável. Em outro sentido, também existe o risco de se definirem requisitos de proteção desnecessários ou de elevado custo de implementação e de manutenção, para proteger uma informação de baixo valor. Essa relação deve ser igualmente evitada.

O questionamento realizado no item 2 buscou identificar a existência ou não de uma metodologia definida e estabelecida para se estimar o valor da informação. Como resposta, a totalidade dos bancos afirmou que não possuem metodologia formalizada com essa finalidade. A inexistência, entre os bancos pesquisados, de uma metodologia para se estimar o valor da informação, provavelmente, se deva à dificuldade de se atribuir valor a um bem intangível. Porém, é importante que cada instituição se esforce em adotar uma metodologia para estimar o valor dos seus ativos informacionais, pois, conhecendo esse valor, o gestor aumentará suas possibilidades de estabelecer requisitos de proteção que guardem compatibilidade com o valor do bem a ser protegido.

Quando se trata de documentos, recomenda-se que esses devem ser guardados ao longo do seu ciclo de vida em diferentes tipos de arquivo, tais como: corrente, intermediário ou permanente. Algumas organizações adotam formalmente a tabela de temporalidade, a qual estabelece o prazo de guarda dos documentos em cada um dos diferentes tipos de arquivo. De modo correlato, o valor da informação também sofre alterações ao longo do tempo. Dessa forma, convém que o gestor conheça e tenha domínio sobre essas alterações. Para tanto, é conveniente utilizar alguma metodologia que possa classificar e oferecer, ainda que de modo estimativo, o valor da informação. Assim, poder-se-á conhecer o tipo de proteção demandada e, também, poder-se-á proteger a informação de maneira mais apropriada. Quando essa atividade não é executada, é como se um documento fosse arquivado em um

tipo de arquivo (corrente, intermediário ou permanente), sem ter sido previamente classificado e permanecesse nesse mesmo arquivo durante todo o seu ciclo de vida.

Mesmo não havendo uma metodologia definida para a estimativa do valor da informação, buscou-se identificar se as instituições faziam distinção entre suas informações. Assim, com base na resposta à questão 2.2, verificou-se que quatro das cinco instituições pesquisadas utilizavam algum critério para classificar suas informações. Dentre os critérios utilizados destacaram-se o agrupamento de informações classificadas como estratégicas, táticas e operacionais ou classificadas como confidenciais, ou ainda, classificadas com base no seu grau de criticidade. Quaisquer desses tipos de classificação já fornecem ao gestor pontos de vista diferenciados da informação. Isso pode subsidiá-lo nas ações de segurança da informação, como, por exemplo, dar tratamento específico para cada grupo de informação de acordo com sua importância.

O questionamento constante no item 3 está relacionado ao retorno do investimento em segurança da informação. Assim, procurou-se identificar se o gestor tem o cuidado de calcular o custo da proteção e compará-lo com o valor atribuído à informação.

Não é razoável se gastar mais com o seguro do que o valor do bem assegurado. As respostas apresentadas ao item 3 indicaram que a maioria das instituições pesquisadas não compara o custo de proteção com o valor da informação protegida. Não obstante, essa é uma atividade de grande importância, pois é a análise financeira da segurança da informação. E, como se sabe, banco, por natureza, visa lucro. Quando essa atividade deixa de ser executada, torna-se difícil garantir que a relação custo da proteção *versus* valor da informação esteja adequada e que o investimento em segurança da informação está tendo retorno satisfatório. Mesmo com os resultados obtidos, não se pode afirmar que os bancos estão atribuindo proteção aquém ou além do valor da informação. Porém, é muito provável que a proteção estabelecida esteja incompatível com o valor da informação.

8.2 Equilíbrio entre os pilares tecnologia, pessoas e processos

O objetivo específico referente aos pilares é estudar a relevância dos pilares tecnologia, pessoas e processos e do equilíbrio entre eles, para se definirem as ações de segurança da informação.

Conforme se detalhou no item 6.2, a metodologia proposta para a análise de cada um dos pilares iniciou-se com a definição das questões e/ou requisitos que deveriam compor cada pilar. A escolha dos requisitos foi diretamente relacionada ao valor da informação que foi objeto da análise. Após essa definição, elaborou-se o questionário e, com o auxílio deste, verificou-se a existência e o grau de atendimento dos requisitos no processo de garantia da segurança da informação.

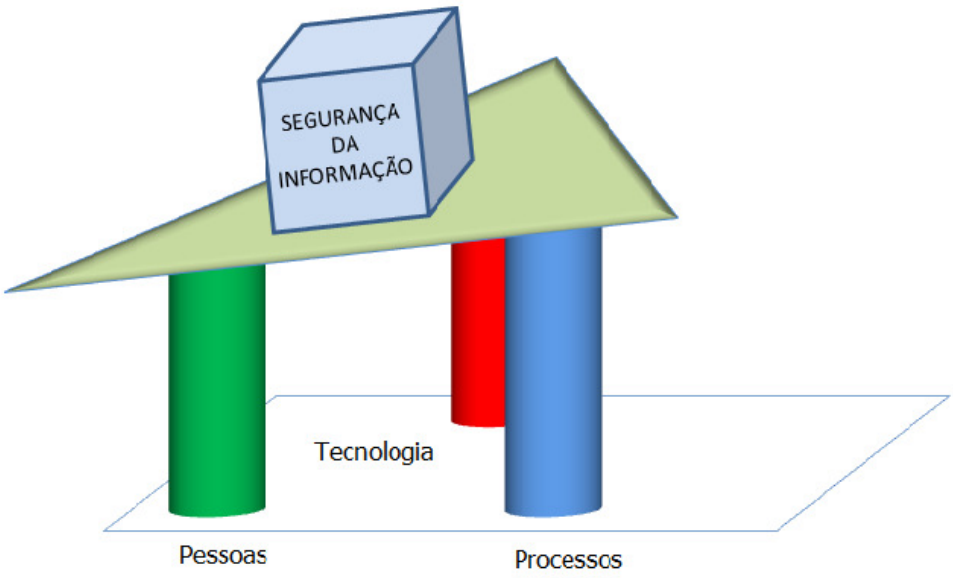
Com as respostas ao questionário aplicado em cada um dos bancos que fizeram parte da amostra desta pesquisa e a tabulação dos respectivos dados, foi possível elaborar as figuras a seguir, que mostram como está cada um dos pilares (tecnologia, pessoas e processos), bem como o equilíbrio entre eles.

A figura 6 mostra os dados do Banco A, de acordo com o ponto de vista do responsável pela segurança da informação daquela instituição:

Figura 6 – Equilíbrio entre os pilares – Banco A

Banco A

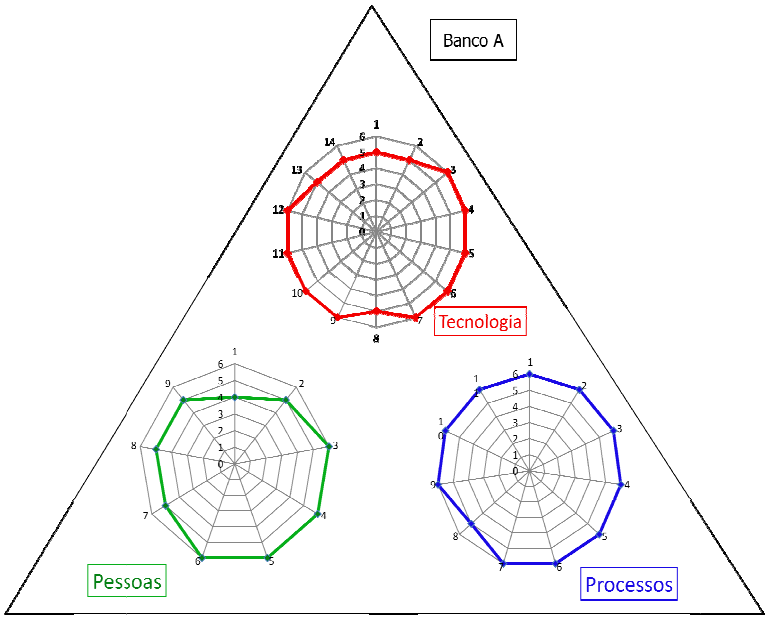
PESSOAS (%)	PROCESSOS (%)	TECNOLOGIA (%)
88,80	98,15	94,01



Observou-se que, nesse banco, o pilar pessoas está ligeiramente menor do que os pilares tecnologia e processos. Dessa forma, foi possível propor um reforço nas questões referentes a pessoas, pois parece que as maiores vulnerabilidades estão acontecendo nesse pilar.

Um melhor detalhamento pôde ser feito a partir de um corte horizontal nos pilares, visando conhecer a estrutura de cada um deles, conforme mostra o gráfico 10.

Gráfico 10 – Estrutura interna dos pilares - Banco A



Nesse gráfico, foi possível verificar a intensidade da existência de cada um dos requisitos definidos para cada pilar, a partir da nota que foi atribuída ao requisito avaliado. As notas variaram de 1 a 6, sabendo-se que 1 indicou que o avaliador discordou totalmente da afirmação de que o requisito estava contemplado de forma satisfatória; e 6 indicou que o avaliador concordou totalmente com a afirmação de que o requisito estava contemplado de forma satisfatória. A escala de avaliação está detalhada nas tabelas 1 e 2, no item 6.2.

Para esse banco, o pilar tecnologia constou de quatorze requisitos, dos quais nove foram avaliados pelo respondente com a nota 6, ou seja, o requisito estava contemplado de forma satisfatória. Os outros cinco requisitos obtiveram nota 5, o que sugeriu a necessidade de reforço deles.

O pilar que necessitou de maior atenção foi o pilar pessoas, no qual, dos nove requisitos avaliados, cinco deles obtiveram notas abaixo do satisfatório.

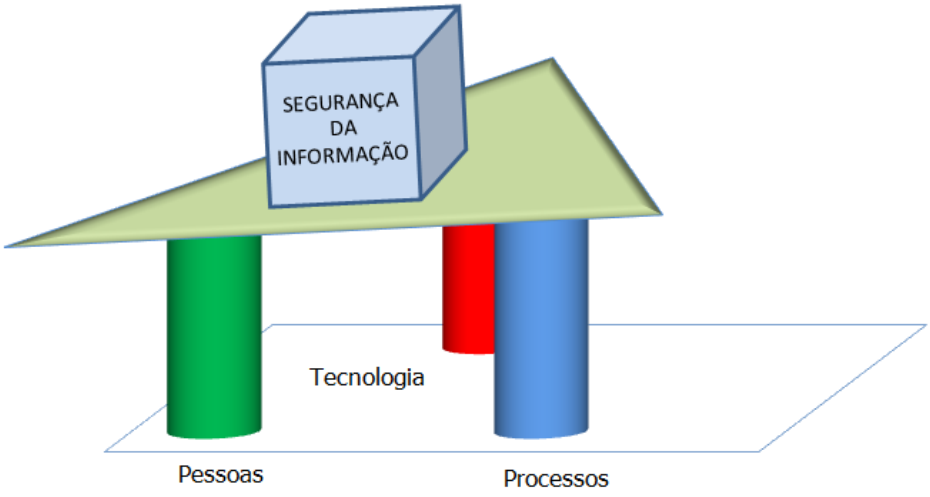
Para se saber quais requisitos precisavam ser reforçados, bastava retornar ao questionário e identificar o número do requisito que obteve nota inferior a 6.

Os pilares que sustentam a segurança da informação no Banco B, de acordo com o ponto de vista do responsável pela área daquela instituição, estavam como mostra a figura 7:

Figura 7 – Equilíbrio entre os pilares - Banco B

Banco B

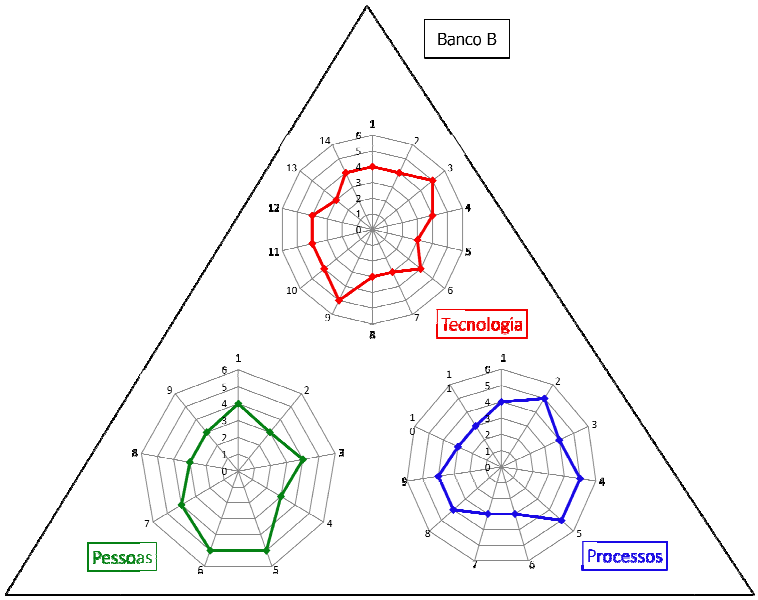
PESSOAS (%)	PROCESSOS (%)	TECNOLOGIA (%)
62,90	64,93	64,26



Também nesse banco, o pilar pessoas estava ligeiramente menor do que os demais pilares, o que sugeriu que esse pilar é o que necessita de maior atenção. No entanto, os demais pilares também necessitam de atenção, pois estavam distantes da posição satisfatória (100%).

Nesse banco, constatou-se uma situação em que os três pilares possuíam tamanhos relativamente próximos um do outro, porém, estavam muito abaixo do desejável 100%. Um olhar superficial pode induzir a uma interpretação equivocada sobre a estabilidade da segurança da informação nos bancos pesquisados, pois, apesar do plano não estar muito inclinado, a estrutura dos pilares estava fragilizada, como se pode ver no gráfico 11.

Gráfico 11 – Estrutura interna dos pilares – Banco B



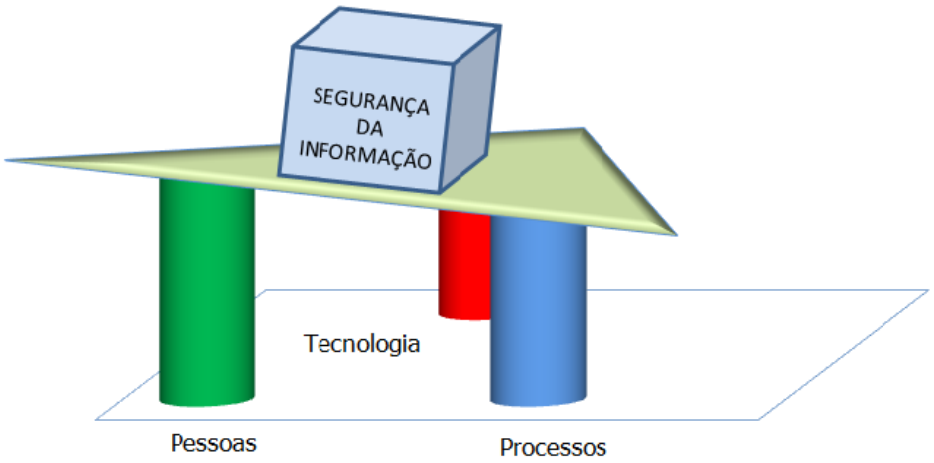
Essa estrutura sugere que os três pilares precisam ser reforçados.

Quanto ao Banco C, o equilíbrio entre os pilares, segundo opinião do responsável pela segurança da informação daquela instituição, encontrava-se conforme registrado na figura 8.

Figura 8 – Equilíbrio entre os pilares – Banco C

Banco C

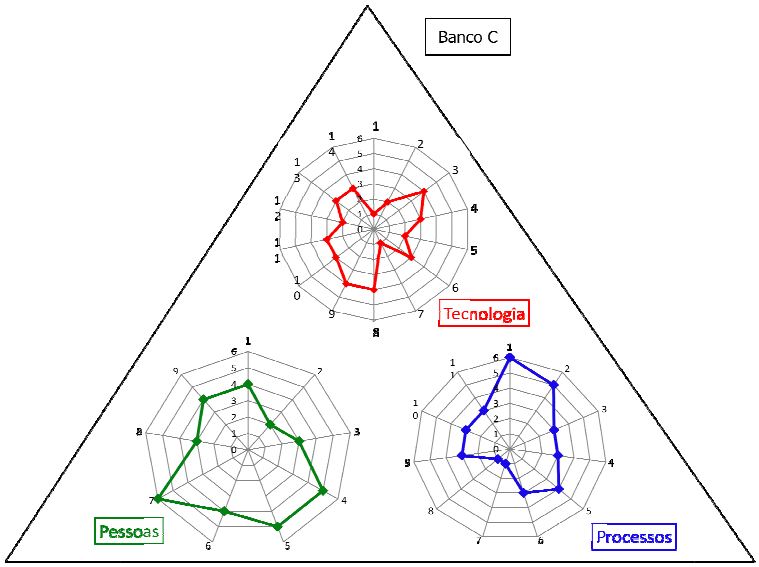
PESSOAS (%)	PROCESSOS (%)	TECNOLOGIA (%)
61,36	52,85	44,03



A situação constatada nos dados dessa instituição é pouco comum, uma vez que o pilar tecnologia, que, historicamente, é o mais atendido em termos de atenção e de investimento, estava bem menor que os demais. Os responsáveis pela segurança da informação naquela instituição acrescentaram a informação de que essa era uma situação de momento, refletida pelas profundas mudanças que estavam acontecendo na área de TI, durante o preenchimento do questionário e, que, tão logo o ambiente de TI retornasse à estabilidade, muito provavelmente, o pilar tecnologia assumiria uma posição satisfatória.

O gráfico 12 mostra o corte horizontal nos pilares do Banco C

Gráfico 12 – Estrutura interna dos pilares – Banco C



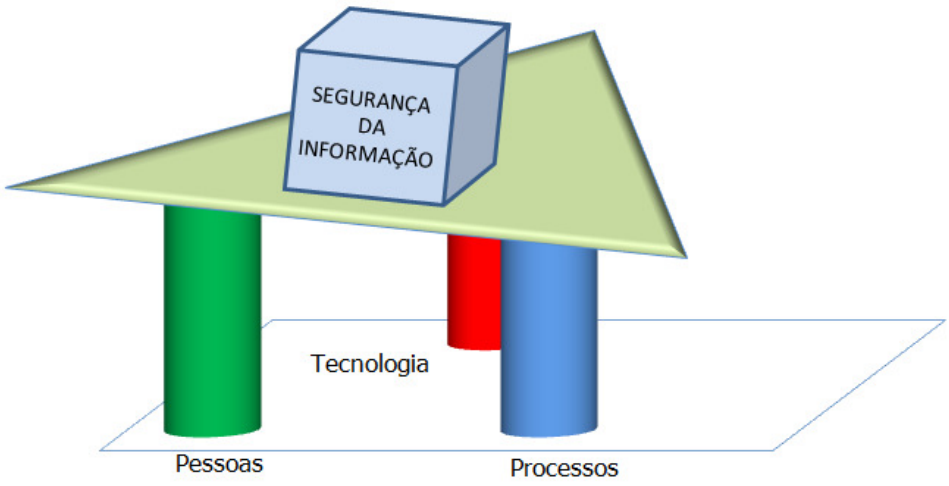
Outra situação importante constatada nos dados dessa instituição foi que o pilar pessoas era o maior dentre os três pilares, o que é incomum. Segundo o respondente, isso se deveu ao forte trabalho de treinamento e de conscientização dos empregados e de terceiros sobre a importância da segurança da informação.

O equilíbrio entre os pilares, segundo a opinião do responsável pela segurança da informação do Banco D, está representado na figura 9.

Figura 9 – Equilíbrio entre os pilares – Banco D

Banco D

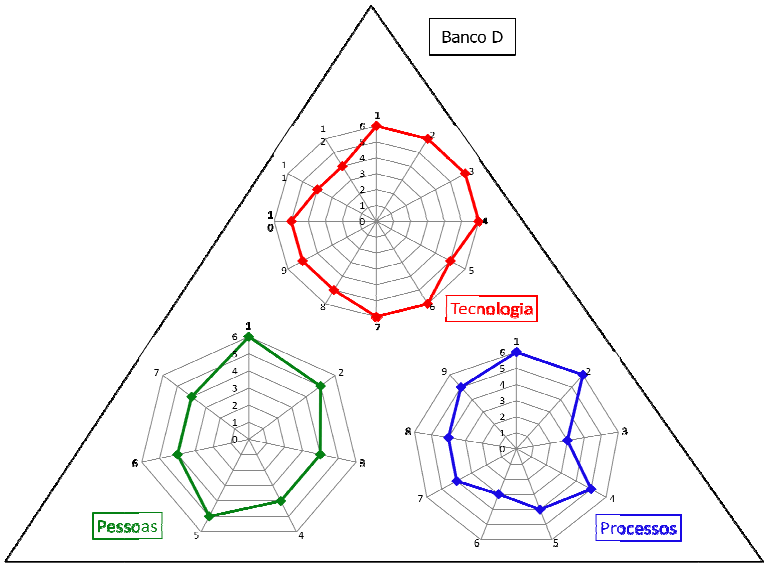
PESSOAS (%)	PROCESSOS (%)	TECNOLOGIA (%)
76,16	74,00	88,96



Nessa instituição, o pilar que obteve a menor pontuação foi o pilar processos, e a tecnologia foi o pilar de maior tamanho. Dessa forma, observou-se o plano inclinado na direção do pilar de menor tamanho, o que sugeriu uma ação prioritária nos requisitos que compunham esse pilar.

O gráfico 13 mostra o corte horizontal nos pilares do Banco D

Gráfico 13 – Estrutura interna dos pilares – Banco D



Observando-se o gráfico 13, é possível perceber que as questões que envolveram tecnologia no Banco D, segundo o respondente, estavam mais bem resolvidas. Nessa instituição, as questões apontadas como críticas e que mereciam intervenção prioritária foram as de números três e seis, do pilar processos. Consultando-se o questionário, constam as seguintes questões:

- Questão 3 - Os requisitos para preservar a confidencialidade das informações estão formalmente definidos e implementados, através de documentos apropriados com funcionários, fornecedores, terceiros e usuários.

- Questão 6 - Os eventos de segurança da informação são relatados através de canais apropriados da direção, o mais rapidamente possível.

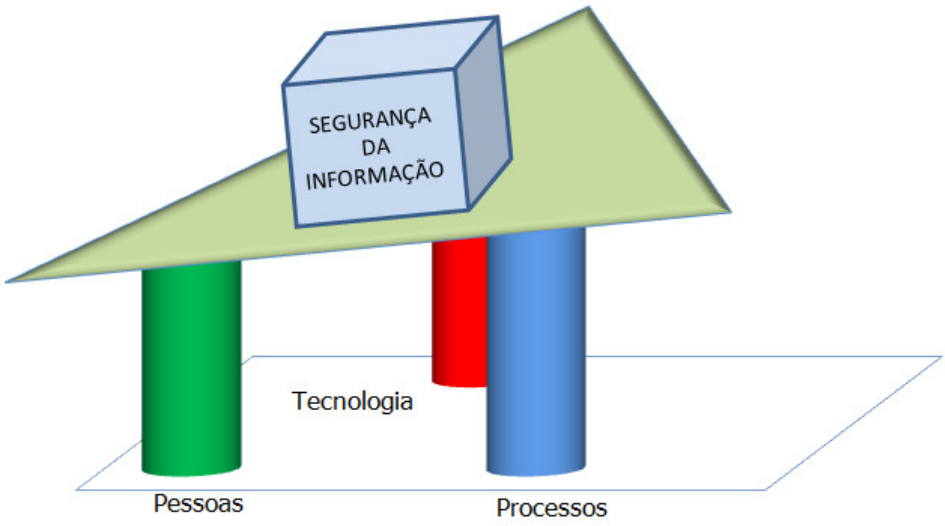
Para essas duas questões, o respondente atribuiu notas muito baixas discordando parcialmente (nota 3) das afirmações constantes nelas.

O equilíbrio entre os pilares, segundo a opinião do responsável pela segurança da informação do Banco E, está representado na figura 10.

Figura 10 – Equilíbrio entre os pilares – Banco E

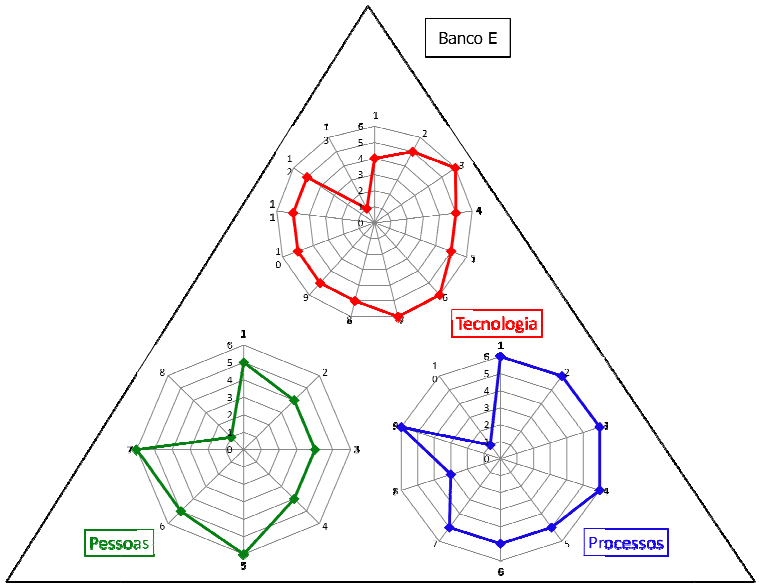
Banco E

PESSOAS (%)	PROCESSOS (%)	TECNOLOGIA (%)
72,80	81,83	80,64



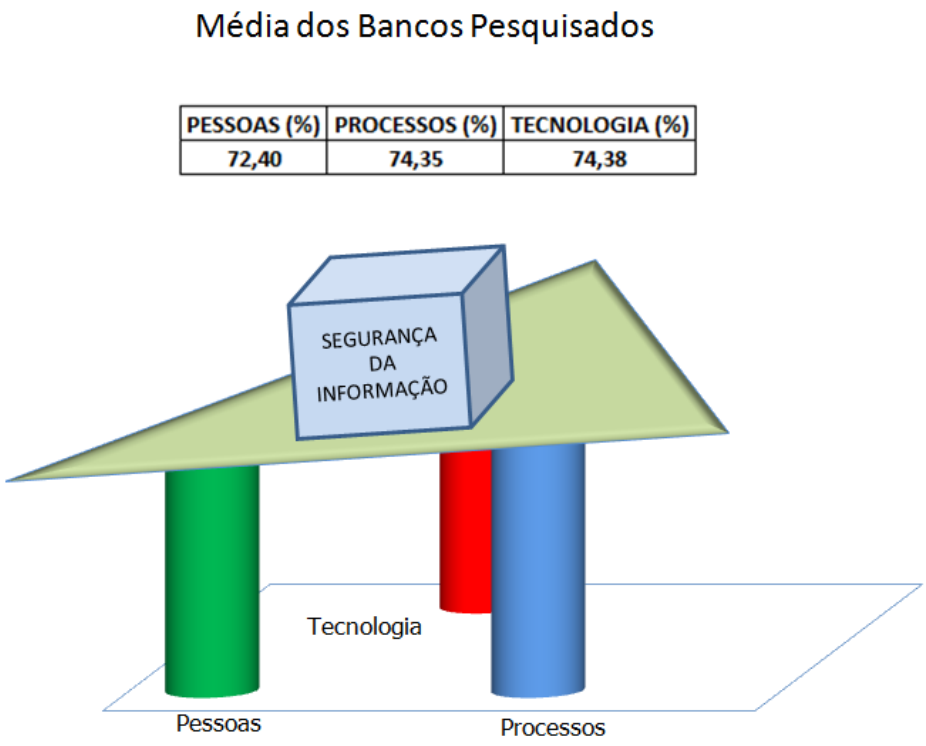
Também no Banco E, o pilar que necessitava de maior atenção era o pilar pessoas. Nesse pilar, os requisitos que requeriam prioridade de intervenção foram os de menor pontuação, como se pode ver no gráfico 14.

Gráfico 14 – Estrutura interna dos pilares – Banco E



Por fim, a figura 11 mostra o tamanho médio de cada pilar e o equilíbrio entre eles.

Figura 11 – Equilíbrio entre os pilares – Média dos bancos pesquisados

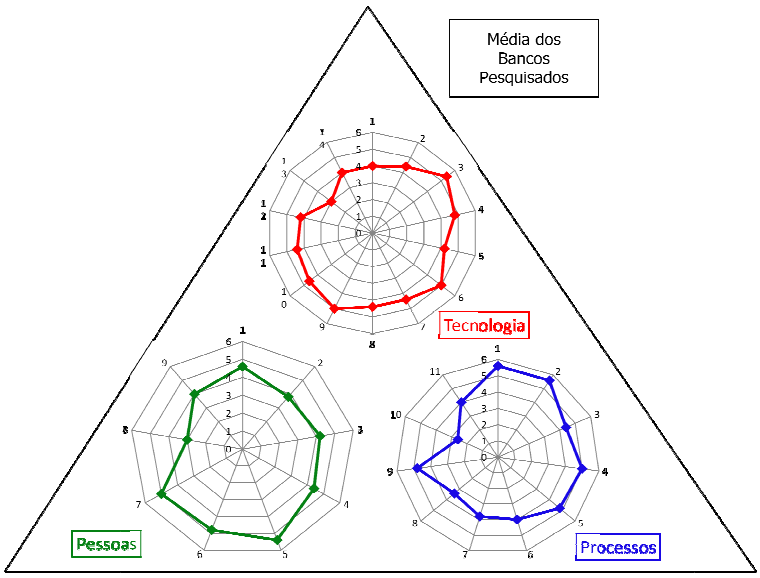


Observou-se que todos os pilares careciam de reforço. Porém, o que necessitava de maior atenção era mesmo o pilar pessoas, o que confirmou as afirmações de tantos autores de que esse é o elo mais fraco da corrente. Também, o pilar tecnologia apareceu, na média, como o mais forte, conforme se esperava, pelo fato de ser, historicamente, o pilar que tem recebido o maior volume de investimento. O pilar processos, na média, estava muito próximo do pilar tecnologia, de acordo com os dados dos bancos pesquisados. Talvez, a forte atuação dos órgãos reguladores e fiscalizadores do setor financeiro possa ter contribuído para essa situação. Por exemplo, a Resolução 3380 do Banco Central do Brasil (BANCO, 2006) determina, em seu artigo 1º, que as instituições financeiras implementem uma estrutura de gerenciamento de risco operacional. O próprio Banco Central define como risco operacional, a possibilidade de ocorrência de perdas resultantes de falhas, de deficiência ou de inadequação de processos internos, de pessoas e de sistemas, ou de eventos externos. Na mesma resolução, o Bacen determina que se realize, com periodicidade mínima anual, testes de avaliação dos sistemas de controle de riscos operacionais implementados. O cumprimento dessas

determinações é verificado, ao menos uma vez ao ano, através de auditoria daquela instituição.

A estrutura interna média dos pilares é apresentada no gráfico 15, a qual explicita quais requisitos de segurança precisam ser reforçados em cada um dos pilares.

Gráfico 15 – Estrutura interna dos pilares – Média dos bancos pesquisados



O requisito de menor pontuação no pilar pessoas foi também o de menor pontuação nos pilares processos e tecnologia, o qual se refere à afirmação de que periodicamente, verificava-se como estava o equilíbrio entre os pilares pessoas, processos e tecnologia. Como essa questão foi a de menor pontuação, significa que os respondentes discordaram dessa afirmação, ou seja, não havia a preocupação, por parte dos gestores, de verificar como estava o equilíbrio entre os pilares. É como se não houvesse nenhuma correlação entre eles.

O segundo ponto que requereu maior atenção no pilar pessoas, de acordo com os respondentes, foi a quantidade insuficiente de pessoal responsável pelos sistemas de segurança da informação, que era inadequada ao porte da empresa e aos riscos a que estava sujeita.

No pilar processos, a segunda maior necessidade de reforço se referia à identificação dos eventos que poderiam causar interrupções aos processos de negócio, bem como o cálculo da probabilidade de tais interrupções ocorrerem, seus respectivos impactos e as consequências para a segurança da informação. Isso está diretamente relacionado à gestão de risco. É a identificação das fragilidades, das ameaças e a definição da resposta ao risco, caso algum incidente venha a ocorrer.

Por fim, no pilar tecnologia, eram vários os pontos que precisavam ser reforçados. No entanto, o item de menor pontuação, e, por conseguinte, que carecia de maior reforço, era a necessidade de se identificar, de maneira precisa, todos os ativos da organização. Além disso, necessitava-se de um inventário estruturado e atualizado desses ativos, bem como da definição formal de regras para o uso deles. Esse é basicamente o ponto de partida: sem inventário atualizado dos ativos e sem regras claras de utilização deles, torna-se quase impossível fazer uma gestão eficaz da segurança da informação.

8.3 Comprovação dos pressupostos

8.3.1 Comprovação do 1º pressuposto

1º pressuposto: O valor da informação é um subsídio importante para se definir os requisitos de segurança da informação.

Os requisitos de segurança que compõem cada pilar (tecnologia, pessoas e processos) têm a função de contribuir para a proteção da informação e devem ser definidos levando-se em consideração o valor da informação.

Para verificar se os bancos pesquisados estavam adotando essa prática, elaborou-se o questionário sobre valor da informação (Apêndice 1), cujas respostas estão explicitadas na tabela 6.

Assim, pôde-se verificar a existência de relação entre o valor da informação e os requisitos de proteção estabelecidos. Essa foi a variável proposta para a comprovação do 1º pressuposto.

Os dados da tabela 6 sugeriram que a maioria dos bancos pesquisados não tem dado importância significativa para a relação entre o valor da informação e os requisitos de proteção estabelecidos. No entanto, não se pôde afirmar que os bancos pesquisados não se preocupavam em estimar o valor da informação, embora a totalidade deles tivesse declarado que não possuía uma metodologia definida e implantada para estimar o valor da informação a ser protegida. Isso ocorreu porque, por outro lado, quatro bancos responderam que utilizavam algum critério para classificarem a informação, tais como: critérios estratégicos (informação estratégica, tática ou operacional); critérios de sigilo (ostensivo, confidencial); critérios de criticidade.

Dos bancos pesquisados, observou-se que o único que estimava o valor da informação antes de definir a sua proteção foi o Banco A. Esse banco foi também o único que, ao definir qual a proteção se daria à informação, tinha-se o cuidado de calcular o custo da proteção e compará-lo com o valor atribuído à informação. Assim, pôde-se evitar que o custo da proteção fosse maior do que o valor da informação protegida.

Para se comprovar melhor o 1º pressuposto, verificou-se se o fato de estimar antecipadamente o valor da informação trazia algum benefício para se definir os requisitos de proteção. Para tanto, aplicaram-se três questionários (Apêndices 2, 3 e 4), cujas respostas ofereceram uma visão de como estava o atendimento, por parte dos bancos pesquisados, aos requisitos de proteção relacionados com pessoas, processos e tecnologia. A tabela 7 mostrou o resultado da tabulação das respostas de cada banco, em termos percentuais de atendimento aos requisitos, ou seja, o tamanho dos pilares pessoas, processos e tecnologia.

Tabela 7 - Tamanho dos pilares dos bancos pesquisados

BANCO/PILAR	PESSOAS (%)	PROCESSOS (%)	TECNOLOGIA (%)
BANCO A	88,80	98,15	94,01
BANCO B	62,90	64,93	64,26
BANCO C	61,36	52,85	44,03
BANCO D	76,16	74,00	88,96
BANCO E	72,80	81,83	80,64
MÉDIA	**72,40**	**74,35**	**74,38**

Observou-se que o banco A foi o que atingiu o maior percentual de atendimento aos requisitos estabelecidos em todos os três pilares. Verificou-se, também, que esse foi o único banco que estimava o valor da informação antes de definir os requisitos de proteção dela. Isso comprovou o 1º pressuposto de que, o valor da informação é um subsídio importante para se definirem os requisitos de segurança da informação. Ou seja, conhecendo o valor da informação o gestor passa a ter elementos que o ajudam a definir mais acertadamente e mais consistentemente os requisitos de proteção da informação. Isso, certamente, contribui para melhorar as ações de segurança da informação.

Além disso, quando se conhece também o custo da proteção, tem-se a possibilidade de compará-lo com o valor estimado da informação e, dessa forma, buscar o melhor retorno do investimento, a fim de evitar que o custo da proteção seja maior do que o valor do ativo protegido.

Pelas respostas obtidas nos questionários aplicados, pareceu-nos que os bancos ainda têm um longo caminho a percorrer no que se refere a: definirem uma metodologia e implementá-la para se estimar o valor da informação; definirem os requisitos de proteção, levando-se em consideração o valor da informação a ser protegida; calcularem o custo de implantação dos requisitos definidos, para que o custo da proteção não seja maior do que o valor da informação.

8.3.2 Comprovação do 2º pressuposto

2º pressuposto: O balanceamento entre os pilares tecnologia, pessoas e processos, contribui para melhoria da segurança da informação.

Cada pilar deve ser composto pelos requisitos de proteção suficientes para garantir a segurança da informação. Esses requisitos devem ser definidos considerando o valor da informação.

Segundo a conclusão da Ernst & Young (2006), esses pilares devem ser cuidadosamente balanceados. Para que haja balanceamento entre os pilares é preciso que os requisitos que os compõem estejam implementados em proporções adequadas e satisfatórias. Como os três pilares são interdependentes, se apenas um ou dois tiver sido bem dimensionados e a implantação deles tiver sido satisfatória, a fragilidade verificada no outro poderá provocar a ruptura de toda a estrutura, o que significa a quebra da segurança da informação. Desta forma, o equilíbrio entre os pilares pode ser um indicador positivo para a melhoria da segurança da informação.

Para comprovar o 2º pressuposto foram aplicados três questionários (Apêndice 2, 3 e 4), cujas respostas foram usadas para mensurar cada um dos pilares. O tamanho dos pilares foi expresso em termos percentuais e mostrou o grau de implementação dos requisitos que os compõem.

A tabela 7 registrou os resultados dos cálculos para o tamanho dos pilares dos bancos pesquisados. Com esses dados foram elaboradas as figuras 6 a 11, as quais revelaram como estava o equilíbrio entre os pilares. Foi constatado que os mesmos possuíam tamanhos diferentes entre si. Os pilares com menor tamanho indicaram a existência de pontos fracos na proteção e sugeriram áreas que necessitavam de intervenção prioritária, a fim de reforçar a segurança da informação.

Entretanto, mesmo que a verificação do equilíbrio seja um indicativo para ações prioritárias de intervenção, sempre poderá existir a falsa impressão de que, se os pilares estiverem em equilíbrio, a segurança pode ter atingido um nível

satisfatório. Isso pode ser razoável quando o equilíbrio entre os pilares ocorrer devido à implantação plena (100%), ou próximo dela, dos requisitos de proteção. No entanto, quando o equilíbrio entre os pilares ocorrer com a implantação dos requisitos em patamares baixos, a proteção poderá estar comprometida. Por isso, convém analisar também a estrutura interna de cada pilar, as quais ficaram demonstradas nos gráficos de 10 a 14.

Esses gráficos revelaram, de maneira muito mais detalhada, os requisitos que careciam de intervenção prioritária, e deram uma indicação mais precisa, dos pontos de controle que deveriam ser reforçados, a fim de contribuir para a melhoria das ações de segurança da informação.

Ao se verificar o grau de implantação dos requisitos tem-se que, quanto menor for a necessidade de intervenção, melhor estará o equilíbrio e, por conseguinte, mais consistente estará a segurança da informação.

A tabela 8 mostrou o tamanho médio dos pilares nos bancos pesquisados, calculados com base nas respostas aos questionários aplicados. Quanto mais próximo de 100% (que representa a implantação plena de todos os requisitos definidos), mais equilibrado estará os pilares e a informação tenderá a estar mais segura.

Tabela 8 – Tamanho médio dos pilares.

BANCO/PILAR	PESSOAS (%)	PROCESSOS (%)	TECNOLOGIA (%)	MÉDIA (%)
BANCO A	88,80	98,15	94,01	93,65
BANCO B	62,90	64,93	64,26	64,03
BANCO C	61,36	52,85	44,03	52,75
BANCO D	76,16	74,00	88,96	79,71
BANCO E	72,80	81,83	80,64	78,42
MÉDIA	**72,40**	**74,35**	**74,38**	**73,71**

Com base nos dados constantes da tabela 8 concluiu-se que o banco com maior equilíbrio entre os pilares foi o banco A, uma vez que foi o banco que necessitava do menor nível de intervenção, demonstrado pela maior média do

tamanho dos pilares (93,65%). Por outro lado, como já tinha sido comprovado no 1º pressuposto, o banco A também foi o banco que demonstrou maior consistência em suas ações de segurança da informação. Desta forma, ficou comprovado o 2º pressuposto de que o balanceamento entre os pilares tecnologia, pessoas e processos, contribui para melhoria da segurança da informação.

9 Discussão das teses

Tese I – A estimativa do valor da informação contribui significativamente para se definirem os requisitos de segurança da informação.

Para se proteger uma informação, é necessário implantar vários requisitos. A escolha dos requisitos a serem utilizados deve basear-se em informações pertinentes e confiáveis. Segundo Hunt (1990), uma decisão vale pela informação que a fundamentou e uma boa decisão estará sempre respaldada por informações consistentes.

Uma das informações fundamentais para se definirem os requisitos de proteção é o valor do ativo que se quer proteger. Estabelecer esses requisitos sem se conhecer ou, no mínimo, estimar qual o valor do bem a ser protegido, é como tomar uma importante decisão, sem fundamentá-la em informações consistentes. Analogamente, é como dimensionar os pilares de uma construção sem se saber qual o peso que eles deverão suportar. Por isso, a quantidade e o tipo de requisito devem estar diretamente relacionados com o valor do bem a ser protegido.

O valor da informação não é a única informação necessária para se definirem os requisitos de proteção. Existem outras, tais como a identificação de ameaças e de vulnerabilidades, porém essas informações não foram objeto de análise deste estudo. No entanto, até mesmo a identificação de ameaças e de vulnerabilidades será mais consistente, quando se conhecer antecipadamente o valor do ativo que se quer proteger.

Os dados da presente pesquisa mostraram que a instituição que obteve a maior nota percentual de implantação dos requisitos em todos os pilares foi

exatamente aquela que declarou que estimava o valor da informação, antes de definir os requisitos de proteção da informação. Isso pôde ser visto na seção 8.3.1, quando se analisou mais detalhadamente os dados da pesquisa e ficou comprovado o 1º pressuposto de que o valor da informação é um subsídio importante para se definirem os requisitos de segurança da informação.

Ao contribuir para a definição mais consistente dos requisitos necessários à proteção da informação, o valor da informação estará igualmente contribuindo para a melhoria das ações de gestão da segurança da informação.

Tese II - A informação tende a estar mais bem protegida quando os pilares tecnologia, pessoas e processos estão em equilíbrio.

Para que uma informação esteja relativamente segura, é necessário que se implementem vários requisitos de proteção. Neste trabalho, esses requisitos foram agrupados conforme sugere Pfleeger (1997), em três segmentos ou pilares: pessoas, tecnologia e processos. Embora os requisitos de proteção constantes na ABNT, NBR ISO/IEC/27.001:2006 (ASSOCIAÇÃO, 2006), norma que trata dos sistemas de gestão de segurança da informação, não estejam classificados dessa forma, pode-se perceber a preocupação em garantir que todos esses aspectos estejam contemplados no texto.

Muito tem se falado da atenção especial dada ao pilar tecnologia, no qual os investimentos têm sido mais significativos, e na pouca atenção dedicada ao pilar pessoas, que é o elo mais fraco da corrente. Nas seções 4.2.4.2 e 4.2.4.3, apresentaram-se vários autores que discutiram o papel fundamental dos processos e das pessoas, e não somente da tecnologia, nas ações de gestão da segurança da informação.

A visão que tem predominado ultimamente é sobre a necessidade de existir equilíbrio entre os segmentos tecnologia, pessoas e processos, como mostra a pesquisa realizada pela Ernst & Young (2006), descrita na seção 4.2.4. Essa pesquisa concluiu que esses pilares são altamente relevantes para a proteção da informação

e, que, por essa razão, devem ser cuidadosamente balanceados, de acordo com a relevância de cada um, na proporção do valor da informação.

Nesse sentido, a segunda tese proposta nesta pesquisa, que sugere que a informação tende a estar mais bem protegida quando os pilares tecnologia, pessoas e processos estão em equilíbrio, é complementar à primeira tese, que sugere que a estimativa do valor da informação contribui significativamente para se definir os requisitos de segurança da informação.

Isso ocorre porque a relevância de cada pilar é definida pelos requisitos que devem compor os pilares. Quando o gestor define esses requisitos na proporção do valor da informação, os pilares ficam bem dimensionados e o balanceamento entre eles certamente trará maior consistência à proteção da informação.

Identifica-se, portanto, três momentos relevantes no processo de gestão da segurança da informação: o primeiro se refere à estimativa do valor da informação; o segundo se refere à definição dos requisitos que serão necessários para proteger a informação; o terceiro se refere à implantação dos requisitos definidos.

A segunda tese aqui proposta, está relacionada com o terceiro momento, e diz respeito à implantação dos requisitos de proteção. O que se argumenta é que, para se garantir a segurança da informação não é suficiente implantar-se, ainda que totalmente, apenas os requisitos de um ou dois pilares.

A representação da segurança da informação apoiada sobre um plano, que é sustentado por três pilares, conforme figura 4 – *Segurança da Informação baseada nos pilares tecnologia, pessoas e processos*, proposta no item 6.1 deste trabalho, mostra claramente a ideia da necessidade de haver equilíbrio entre os pilares. Quando os pilares não estão em equilíbrio o plano se inclina, e, como consequência, expõe a informação a riscos oriundos, oportunistamente, das

fragilidades do menor pilar, o que pode provocar, com maior facilidade, a quebra da segurança da informação.

Desta forma, é conveniente que se busque manter os pilares que sustentam a segurança da informação em equilíbrio, pois isso, muito provavelmente, aumentará as possibilidades de se ter a informação mais bem protegida.

10 Conclusões

Após a revisão de literatura sobre os assuntos tratados neste trabalho, o lançamento dos pressupostos e das variáveis, a realização da pesquisa de campo, a análise dos dados coletados e a proposição das teses, pôde-se chegar às seguintes conclusões:

A. Com relação à necessidade de proteção da informação:

- A informação estratégica tem adquirido importância tão elevada, a ponto de se tornar, na maioria das vezes, o principal ativo de uma organização e, até mesmo, de nações, uma vez que o uso da informação pode determinar o grau de sucesso ou de fracasso da organização.

- Ao assumir a condição de ativo de alto valor estratégico, a informação precisa ser tratada de forma condizente com sua relevância, ser revestida de cuidados especiais e protegida adequadamente.

B. Com relação ao valor da informação:

- A informação estará mais adequadamente protegida se os requisitos de proteção dela forem compatíveis com o seu valor. Para tanto, é fundamental que se estime o valor da informação antes de se definirem quais serão os recursos utilizados para protegê-la. É nesse sentido que o valor da informação pode fornecer importante subsídio no processo de gestão da segurança da informação.

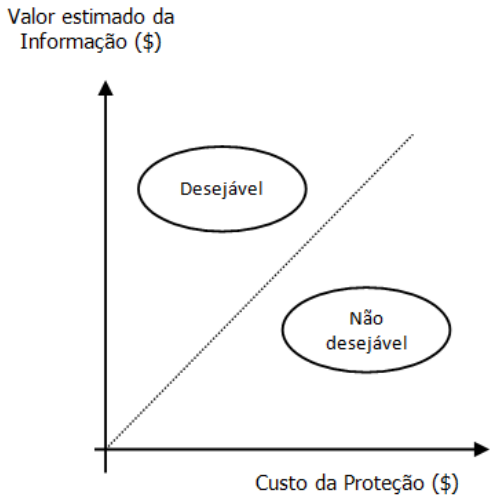
- Valor da informação é aquilo que a informação possui e que a torna relevante em um processo de tomada de decisão. Esse valor está associado à potencialidade do uso e ao grau de sigilo da informação. Nesse caso, é o usuário que deve perceber e estimar o valor da informação, pois é ele que tem a dimensão da utilidade da informação.

- As instituições bancárias pesquisadas demonstraram dificuldades para estimar o valor da informação e eram poucas as que usavam uma metodologia para realizar essa tarefa. Desta forma, os requisitos de proteção não estavam sendo definidos, ao menos metodologicamente, com base no valor da informação, muito embora, empiricamente, o gestor procurasse levar em consideração a relevância da informação a ser protegida.

- Também, na grande maioria das vezes, não se verificou a compatibilidade entre o valor da informação e o custo de proteção dela. Esses dados são fundamentais para se calcular o retorno do investimento em segurança. Não os conhecendo, também não se poderá verificar qual o retorno está se obtendo com o investimento realizado.

- A relação entre o valor da informação e o custo da proteção dela deve ser um ponto de maior atenção pelo gestor, que poderá utilizar um gráfico, semelhante ao gráfico 16, para plotar os dados relativos ao valor da informação e ao custo da proteção dela. É desejável que o ponto de interseção das duas variáveis esteja acima da linha diagonal, uma vez que, quando isso não ocorrer, significa que o custo da proteção da informação está maior do que o valor da informação. Nessas circunstâncias, é melhor, financeiramente, assumir o risco da quebra da segurança da informação.

Gráfico 16 - Valor estimado da informação *versus* custo da proteção



C. Com relação aos pilares que sustentam a segurança da informação:

- A definição dos requisitos de proteção que compõem os pilares tecnologia, pessoas e processos deve levar em consideração o valor da informação e os riscos a que ela está sujeita.

- De maneira geral, constatou-se que era preciso reforçar todos os pilares que sustentavam a segurança da informação, já que não foi possível identificar sequer um banco, cujos requisitos de proteção tivessem completamente implementados.

- O pilar pessoas continua sendo o que recebe menor atenção. Isso confirma o resultado de pesquisas de outros autores e, por conseguinte, é o pilar que carece de maior investimento.

- O pilar tecnologia foi o que obteve a maior pontuação média entre os pilares. Todavia, não se pode descuidar desse pilar, uma vez que ainda existem vários requisitos de proteção que não foram totalmente implementados, conforme se pôde ver no gráfico 15. Tais requisitos precisavam ser reforçados.

- O pilar processos apresentou resultado muito próximo do resultado do pilar tecnologia. Isso demonstrou estar havendo maior preocupação dos gestores em relação: à governança corporativa; à formalização e à implantação de política de segurança da informação; à definição formal de papéis e de responsabilidades de empregados e de terceiros; à monitoração de incidentes de segurança; à elaboração e à implantação de planos de continuidade de negócios, entre outros. No segmento bancário, a atuação dos órgãos reguladores e fiscalizadores, provavelmente tenha contribuído positivamente para essa melhoria.

- A preocupação em tratar os pilares de maneira conjunta ainda era muito baixa por parte dos gestores. Não se verificava periodicamente como estava o equilíbrio entre os pilares pessoas, processos e tecnologia. Cada pilar estava sendo tratado isoladamente, como se não houvesse interseção entre eles. Porém, como os sistemas de informação são formados por pessoas, processos e tecnologia, para protegê-los é necessário atuar nessas três dimensões, simultaneamente, pelo fato de serem interdependentes. Não é suficiente dimensionar bem os requisitos de proteção e implementá-los plenamente em um ou em dois pilares e deixar o outro subdimensionado. A estrutura se romperá no pilar mais frágil, não importa qual seja. Dessa forma, convém que os três pilares sejam dimensionados de forma integrada, considerando-se que estão interligados e são interdependentes entre si. Além disso, a implementação dos requisitos de proteção deve ser feita de forma a preservar o equilíbrio entre a tecnologia, as pessoas e os processos.

- A informação estará mais bem protegida quando os requisitos de proteção forem definidos, levando-se em consideração o valor da informação e a implementação desses requisitos se der de forma a preservar o equilíbrio entre os pilares tecnologia, pessoas e processos. Isso pôde ser comprovado analisando-se as respostas do Banco A, que

teve a melhor relação entre o valor da informação e os requisitos de proteção. Esse foi o único banco que declarou cuidar para preservar o equilíbrio entre os pilares.

11 Limitações do estudo

Toda vez que se pretende pesquisar sobre segurança da informação nas instituições, o pesquisador depara-se com a afirmação de que esse assunto é sigiloso e que as informações são confidenciais. Dessa maneira, é muito difícil coletar grande quantidade de informações, ou mesmo, testar uma metodologia que necessite de dados considerados confidenciais. As organizações têm receio de revelar suas fragilidades, mesmo em trabalhos eminentemente acadêmicos. O vazamento de informações de segurança pode provocar forte impacto negativo na imagem da instituição no mercado e a desconfiança do seu cliente, o que normalmente se traduz em perdas financeiras.

Para conseguir os dados necessários à realização desse trabalho foi decisiva a preservação das fontes, com compromisso formal de confidencialidade. Por isso, as fontes foram tratadas apenas como Banco A, Banco B, Banco C, Banco D e Banco E. No entanto, mesmo preservando as fontes, não foi possível obter informações sobre o número de incidentes de segurança ocorridos no período pesquisado. O argumento das instituições sobre isso foi que essa é uma informação ultraconfidencial. Assim, esses dados não puderam ser analisados.

Outra limitação desse estudo é que a pesquisa de campo colhe a opinião do respondente sobre questões previamente colocadas. Embora o respondente tenha sido selecionado para a enquete por ser um profundo conhecedor de sua instituição e dos assuntos abordados na pesquisa, nem sempre sua opinião correspondeu à realidade da organização. Assim sendo, em um trabalho mais aprofundado, como acontece em auditorias, é conveniente solicitar evidências das respostas dadas.

A solicitação de evidências não permitiria que um respondente afirmasse, por exemplo, que "Os funcionários, os fornecedores, os terceiros e os usuários recebem, periodicamente, treinamento apropriado sobre as questões de segurança da informação...", sem apresentar os devidos comprovantes dos treinamentos, tais como: resenha dos cursos, material didático utilizado, listas de presenças, avaliações dos participantes, entre outros.

Porém, se tivesse sido exigida a comprovação de cada uma das respostas aos itens dos questionários aplicados, não teria sido possível realizar esta pesquisa. De todo modo, quando for possível verificar a veracidade das respostas, a tendência é que os resultados obtidos com a tabulação dos dados se aproximem muito mais da real situação da organização.

12 Sugestão para novas pesquisas

Este trabalho de pesquisa não teve a pretensão de esgotar o tema, sobretudo devido à alta complexidade das questões estudadas, e também pelo fato de o assunto tratado permear diversas áreas do conhecimento, com alcance nas atividades da iniciativa pública e da iniciativa privada. Além disso, o tema pode ser visto, discutido e analisado, a partir de diferentes perspectivas, as quais, mesmo depois de serem estudadas exaustivamente, ainda continuarão necessitando de aprofundamento. Por isso, a pesquisa talvez possa ter a pretensão de contribuir para melhorar o entendimento sobre as questões de segurança da informação e/ou ser um ponto de partida para outras discussões sobre esse assunto.

Assim, com o objetivo de dar continuidade ao ciclo de construção e de consolidação do conhecimento, especificamente, visando tornar as ações de segurança da informação mais eficazes, visualizamos a possibilidade de novos estudos com as seguintes abordagens:

- Estudo das razões pelas quais poucos gestores estão estimando o valor da informação como subsídio para se definirem os requisitos de proteção da informação. Será por falta de uma metodologia prática que

facilite a execução da tarefa, ou será porque os gestores ainda não entenderam os benefícios dessa etapa, para a gestão da segurança da informação?

- Proposição de uma metodologia que possa auxiliar o gestor a estimar o valor da informação que se pretende proteger.

- Aprofundamento de estudos sobre segurança da informação nos limites de abrangência da ciência da informação.

- Estudo comparativo entre os indicadores de segurança da informação, antes e depois de intervenções para as devidas correções dos requisitos de proteção que compõem os pilares tecnologia, pessoas e processos.

- Pertinência da inserção de diferentes pesos nos pilares tecnologia, pessoas e processos, quando da verificação do desejado equilíbrio entre eles nos requisitos de segurança da informação.

Referências

ALBERTS, Christopher *et al*. **Introduction to the OCTAVE® Approach.** Pittsburg: Carnegie Mellon University, 2003. 37 p.

AMARAL, Luis Alfredo Martins do. **PRAXIS:** um referencial para o Planejamento de Sistemas de Informação. 1994. Tese (Doutorado) - Departamento de Sistemas de Informação, Universidade do Minho, Guimarães (Portugal), 1994. Disponível em: https://repositorium.sdum.uminho.pt/retrieve/301/PRAXIS_Amaral.pdf. Acesso em: 28 mai. 2011.

ANDRADE, Dalton Francisco de Andrade; TAVARES, Heliton Ribeiro; VALLE, Raquel da Cunha. **Teoria da Resposta ao Item**: conceitos e aplicações. São Paulo: Associação Brasileira de Estatística, 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ISO IEC 27001:** Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2006. 34 p.

_____. **ISO/IEC 2000-1:2005 – Information Technology – Service Management:** Part 1: Specification. Rio de Janeiro: ABNT, 2005.

_____. **NBR ISO 9001:2008** - Sistemas de gestão da qualidade – Requisitos. Rio de Janeiro: ABNT, 2008.

_____. **NBR ISO/IEC 12207:1998** – Tecnologia de Informação – Processos de Ciclo de Vida de Software. Rio de Janeiro: ABNT, 1998.

_____. **NBR ISO/IEC 17799:2005** - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. 2.ed. Rio de Janeiro: ABNT, 2005.

_____. **NBR ISO/IEC 27001:2006** – Tecnologia da Informação: Técnicas de segurança - Sistema de Gestão da Segurança da Informação – Requisitos. Rio de Janeiro: ABNT, 2006.

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

_____. **NBR ISO/IEC 9126-1: 2003 -** Engenharia de software - Qualidade de produto Parte 1: Modelo de qualidade. Rio de Janeiro: ABNT, 2003.

_____. **NBR ISO 9001: 2000 –** Sistemas de gestão da qualidade. Rio de Janeiro: ABNT, 2000.

AYTES, Kregg; CONOLLY, Terry. A Research Model for Investigating Human Behavior Related to Computer Security. In: AMERICAS CONFERENCE ON INFORMATION SYSTEMS, 9., 4-62003, Tampa, Fl, USA. **Proceedings...** Tampa, Fl, USA: AMCIS, 2003. p. 2027 - 2031. Disponível em: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1726&context=amcis2003. Acesso em: 15 out. 2010.

BALTZAN, Paige; PHILLIPS, Amy. **Sistemas de Informação**. McGraw-Hill Education em parceria com AMGH Editora. Porto Alegre, 2012.

BANCO CENTRAL DO BRASIL. Resolução nº 3380, de 29 de junho de 2006. Dispõe sobre a implementação de estrutura de. **Diário Oficial da União**. 125 Brasília, DF: Imprensa Nacional, 3 jul. 2006. Seção 1, p. 15. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=15&data=03/07/2006>. Acesso em: 17 mar. 2013.

BANERJEE, Debasish; CRONAN, Timothy Paul; JONES, Thomas W. Modeling IT Ethics: a study in situational ethics. **MIS Quarterly**, Minnesota, v. 22, n. 1, p.31-60, mar. 1998. Disponível em: http://misq.org/modeling-it-ethics-a-study-in-situational-ethics.html. Acesso em: 15 out. 2010.

BATES, Marcia. J. The invisible substrate of information science. **Journal of The American Society for Information Science**, v. 50, n.12, p. 1043-1050, 1999.

BBC, UK. Especialistas temem guerra cibernética no futuro, 2012. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2012/04/120430_cyberguerra_futuro_fn.shtml. Acesso em: 25 out. 2012.

BEATSON, John G. Security - a personnel issue: the importance of personnel attitudes and security education. In: INTERNATIONAL CONFERENCE ON COMPUTER SECURITY, 60th. **Proceedings...** Helsink: International Federation For Information Processing, 1991.

BECK, U. Risk society. **Towards a new modernity**. Londres: Sage Publications, 1992.

BORKO, H. Information science: what is it? **American Documentation**, Washington, v.19, n.1, p.3-5, jan. 1968.

BRASIL. **Lei nº 9296 de 24 de julho de 1996**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 17 mar. 2013.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 18 novembro de 2011. Disponível em: http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1000&pagina=1&data=18/11/2011. Acesso em: 17 mar. 2013.

BRASIL. **Leis Complementar nº 105 de 10 de janeiro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 17 mar. 2013.

BRAY, Thomas J. Security actions during reduction in workforce efforts: what to do when downsizing. **Information system security**, v.11, n. 1, p. 11-15, 2002.

BRENNAN, Richard P. **Gigantes da física**. Jorge Zahar Editor Ltda, 2000.

BURK, Cornelius Franklin; HORTON, Forest W. **InfoMap**: a complete quide to discovering corporate information resources. New York: Englewood Cliffs/Prentice Hall, 1988. 254 p.

BUSH, Vannevar. As we may think. **The Atlantic Monthly**, Boston, v. 176, n. 1, p. 101-108, 1945. Disponível em: http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/. Acesso em: 08 mar. 2009.

CARVALHO, Dermeval Bicalho; SANTOS, GUSTAVO MARTINS DOS. **Os Acordos de Basiléia**: um roteiro para implementação nas instituições financeiras. Disponível em: http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Artigo_Basileia_6.pdf. Acesso em: 11 jun. 2013.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.br. Núcleo de Informação e Coordenação do Ponto BR. **Estatísticas dos incidentes reportados ao CERT.br**. Disponível em: www.cert.br/stats/incidentes. Acesso em: 20 mar. 2014.

CERT - SOFTWARE ENGINEERING INSTITUTE. **CERT Statistics (Historical).** Disponível em: www.cert.org/stats/cert_stats.html. Acesso em: 27 jun. 2010.

CESAR, Ricardo. A bola de neve digital: as vendas de PCs podem superar as de televisores neste ano -- e o impacto já se faz sentir. **Exame.com,** São Paulo, v. 2, n. 22, p.1-4, 22 fev. 2007. Semanal. Disponível em: <http://exame.abril.com.br/noticia/a-bola-de-neve-digital-m0123090>. Acesso em: 25 mai. 2012

CHAUMIER, J. **Systemes d'information**: marché et technologies. Paris: Enterprise Moderne, 1986.

CHOO, Chun Wei. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. 2. ed. São Paulo: SENAC, 2003. 425p

CHOO, Chun Wei. **Information management for the intelligent organization**: the art of scanning the environment. 2. ed. [s. l.: ASIS], 1998.

CLARKE, Richard A. **Cyber war**: the next threat to national security and what to do about it. Ecco, 2010.

CLUSTERS: segurança estratégica. **Tema**, v.33, n.198, maio/jun.2009. Disponível em: http://www4.serpro.gov.br/imprensa/publicacoes/tema-1/antigas%20temas/tema-198/materias/clusters. Acesso em: 13 jun. 2013.

CONDON, E.U. Science and security. **The American Biology Teacher**, v. 10, n.4, pp. 107-108, apr. 1948.

COOK, C.; HEATH, F.; THOMPSON, R. L. A meta-analysis of response rates in Web-or Internet-based surveys. **Educational and Psychological Measurement**, Durham, v. 60, n. 6, p. 821-836, Dec. 2000.

COX, Andrew; CONNOLY, Sarah; CURRAL, James. Raising information security awareness in the academic setting. **Vine**: The Journal of Information and Knowledge Management Systems, Bingley, Uk, v. 31, n. 2, p.11-16, 2001.

CRONIN, Blaise. Esquemas conceituais e estratégicos para a gerência da informação. **Revista da Escola de Biblioteconomia da UFMG**, v. 19, n. 2, p. 195-220, set. 1990.

CSI/FBI, Tenth annual computer crime and security survey. Computer Security Institute, 2005.

CUNHA, M.; CAVALCANTI, C. **Dicionário de Biblioteconomia e Arquivologia**. Brasília: Briquet de Lemos. 2008.

DAVENPORT, E., CRONIN, B. Competitive intelligence and social advantage. **Library Trends**, v. 43, n. 2, p. 239-52, Fall, 1994.

DAVENPORT, Thomas H. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DAVENPORT, Thomas H.; MARCHAND, D. A. **Dominando a gestão da informação**. Porto Alegre: Bookman, 2004.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000. 218p

DREYFUSS, Cassio. **As redes e a gestão das organizações**. Rio de Janeiro: Guide, 1996.

DRUCKER, Peter. **Sociedade pós-capitalista**. São Paulo: Pioneira, 1993.

DUNN, M.D. A method to estimate the value of well log information. In: SPE ANNUAL TECHINICAL CONFERENCE AND EXHIBITION, 4-7 de outubro de 1992, Washington. **Proceedings... .** Washington: Society of Petroleum Engineers, 1992.

ELLWANGER, Cristiane. **Impacto da utilização de técnicas de endomarketing na efetividade das políticas de segurança da informação.** 2009. 134 f. Dissertação (Mestrado) – Programa de Pós-Graduação em Engenharia de Produção. Centro de Tecnologia. Universidade Federal de Santa Maria, 2009.

ERNST & YOUNG TERCO. **Pesquisa global sobre segurança da informação:** 2006. Disponível em www.ey.com.br. Acesso em: 23 mar. 2010.

ESTADOS UNIDOS. Department of Defense. **Trusted computer system evaluation criteria**. Washington, 1985. Disponível em: http://m.tech.uh.edu/faculty/conklin/IS7033Web/7033/RainbowSeries/Rainbow%20Series%20Library.htm. Acesso em: 12 fev. 2012.

ESTADOS UNIDOS. Health insurance portability and accountability act of 1996. **Public Law** 104-191, Aug. 21, 1996.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Segurança**: um compromisso de bancos e clientes, 2004. Disponível em www.febraban.org.br. Acesso em: 12 set. 2012.

FERNANDES, Jorge H.C.; **Segurança da informação**: Nova disciplina na ciência da informação? XI Encontro Nacional de Pesquisa em ciência da informação. Rio de Janeiro, 2010.

FORCHT, Karen A.; PIERSON, Joan K.; BAUMAN, B.M.. Developing awareness of computer ethics. In: SIGCPR CONFERENCE ON MANAGEMENT OF INFORMATION SYSTEMS PERSONNEL, 1988, New York. **Proceedings... .** New York: Association For Computing Machinery, 1988. p. 142 - 143.

FREITAS, Marcos A. S. **Fundamentos do Gerenciamento de Serviços de TI**: Preparatório para a certificação ITIL® Foundation. 2.ed. Rio de Janeiro: Brasport, 2011. 424 p., 2011.

FUSCO, Camila; PAIVA, Natália. Vazamento pode custar US$ 2 bi à Sony. **Folha de São Paulo.** São Paulo, 4 maio 2011. Mercado, p. 1. Disponível em: <(http://www1.folha.uol.com.br/fsp/mercado/me0405201103.htm)>. Acesso em: 11 maio 2012.

GABBAY, M. S. **Fatores influenciadores da implementação de ações de gestão da informação**: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte. Natal: Universidade Federal do Rio Grande do Norte, 2003.

GORDON, Lawrence A. *et al*. **Computer Crime and Security Survey.** San Francisco, CA: Computer Security Institute/Federal Bureau of Investigation's, 2005. Disponível em: http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf. Acesso em: 27 abr. 2010.

HAGEN, J. M. *at al.* Implementation and effectiveness of organizational information security measures. **Information Management & Computer Security**, v.16, n. 4, p. 377-397, 2008.

HAMMER, Michael, CHAMPY, James. **Reengineering the corporation**. New York: Harper Business, 1994.

HAMMER, Michael. **A empresa voltada para processos**. Management, jul./ago. 1998. (Entrevista).

HAMMER, Michael. **Towards the twenty-first century enterprise**. Boston: Hammer & Co., 1996. (Folheto).

HUNT, Charles; ZARTARIAN, Vahé. Le renseignement stratégique au service de votre entreprise. Paris: First, 1990. IN: SANTOS, Raimundo Nonato Macedo dos. Métodos e ferramentas para gestão de inteligência e do conhecimento. **Perspect. cienc. inf.**, Belo Horizonte, v. 5, n. 2, p. 205 - 215, jul./dez.2000.

IDC Releases. **Vendas de tablets no segundo trimestre superam 1,9 milhão de unidades, com crescimento de 151% em relação a 2012**. São Paulo: IDC Brasil, 2013. Disponível em: http://br.idclatin.com/releases/news.aspx?id=1510. Acesso em: 05 ago. 2013.

IDGNOW, Hackers prometem novo ataque contra Sony. Disponível em: (http://idgnow.com.br/seguranca/2011/05/06/hackers-prometem-novo-ataque-contra-sony-afirma-site/). Acesso em: 07 dez. 2013.

IMONIANA, Joshua O. Validação de modelos de políticas de segurança da informação. **Transinformação**, Campinas, 16(3) :263-274, setembro/dezembro, 2004.

INFORMATION Security Breaches Survey. Technical Report, 2008. UK: Department for Business Enterprise & Regulatory Reform (BEER), 2008. Disponível em: http://www.bis.gov.uk/files/file45714.pdf. Acesso em: 27 abr. 2010.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. **ITGI**. Information Security Governance: Guidance for Boards of Directors and Executive Management. 2006. 2a. Edition. Disponível em: <http://www.itgi.org>.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001** (BS 7799-2). Information technology. Security techniques. Information security management systems – requirements, Britain: ISO, 2005.

IT GOVERNANCE INSTITUTE. **COBIT 4.1**. Illinois, 2007.

KING, J. L.; SCHREMS, E. L. Cost-benefit analysis in information systems development and operation. **Computing Surveys**, v. 10, p.19-34, 1978.

KRAUSE, Micki; TIPTON, Harold F. **Handbook of information security management**. Florida, USA: Auerbach Publications, 1999.

LANDWEHR, Carl E. Computer Security. **International Journal of Information Security,** v. 1, n. 1, p. 2-13, aug. 2001.

LATHAM, Donald C.. **Department of Defense Trusted Computer System Evaluation Criteria. Washington,USA:** Department of Defense, 1985. Disponível em: http://csrc.nist.gov/publications/history/dod85.pdf. Acesso em: 04 maio 2010.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação gerenciais.** São Paulo: Pearson Prentice Hall, 2007.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**: com Internet. Rio de Janeiro: LTC, 1999.

LAURINDO, Fernando J. B. *et al*. O papel da Tecnologia da Informação (TI) na estratégia das organizações. **Gestão & Produção** v.8, n.2, p.160-179, ago. 2001;

LE COADIC, Yves-François. **A ciência da informação**. 2. ed. Brasília: Briquet de Lemos/Livros, 2004.

LE COADIC, Yves-François. **A ciência da informação**. Brasília: Briquet de Lemos/Livros, 1996.

LESCA, H.; ALMEIDA, F. C. Administração estratégica da informação. **RAUSP**. São Paulo, v.29, n.03, p.66-75, jul./set., 1994.

LIKERT, R. A technique for the measurement of attitudes. **Arch.Psychol,** n.140, p.1-55, 1932.

LORENS, Evandro. **Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação.** 2007. 128 f. Dissertação (mestrado) - Faculdade de Economia, Administração, Contabilidade e ciência da informação e Documentação, Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília. 2007.

MARCIANO, João Luiz Pereira. **Segurança da informação:** uma abordagem social. 2006. 211 f. Tese (doutorado) - Faculdade de Economia, Administração, Contabilidade e ciência da informação e Documentação, Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília. 2006.

MARTINS, A.; ELOFF, Jan H. P. Information security culture. In: INTERNATIONAL CONFERENCE ON INFORMATION SECURITY: VISIONS AND PERSPECTIVES, 17., 2002, The Netherlands. **Proceedings... . Devender,** The Netherlands: Kluwer, B.V., 2002. p. 203 - 214.

MATTAR, F. **Pesquisa de Marketing**. Atlas: 2001.

McDANIEL, George. IBM Dicitionary of Computing. New York, NY: McGraw-Hill, 1994.

McGEE, J. & PRUSAK, L. **Gerenciamento estratégico da informação**. 10. ed. Rio de Janeiro: Campus, 1994.

MENEZES, Silvio Farias de. **Proposta de um modelo de avaliação da segurança da informação nas organizações centrada no usuário.** Recife, 2008. 60 f. Dissertação (mestrado) - Universidade Federal de Pernambuco. 2008.

MOBILE WORLD CONGRESS. Barcelona, 2010.

MÓDULO: Tecnology for Risk Management. **Pesquisa Nacional De Segurança Da Informação, 10**. 2006. Disponível em: http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf. Acesso em: 15 maio 2011.

MOODY, Daniel; WALSH, Peter. Measuring the value of information: an asset evaluation approach. **Proceedings**... European Conference on Information Systems, 7, Copenhagen Business School, Frederiksberg, Denmark, 23-25 June, 1999. Disponível em: http://wwwinfo.deis.unical.it/~zumpano/2004-20005/PSI/lezione2/ValueOfInformation.pdf. Acesso em: 10 mar. 2010.

MURRAY B. Running corporate and national security awareness programmes. In: International Conference on Information Security, 7. 1991. Brigton. **Proceedings**... . Brigton: Elsevier, 1991. p. 203-207

NNOLIM, Anene. L. A **framework and methodology for information security management**. 2007. Tese (doutorado) - Lawrence Technological University - USA, 2007.

O'BRIEN, James A. **Sistemas de informação e as decisões gerenciais na era da internet**. 3.ed. São Paulo: Saraiva, 2001.

OLIVEIRA, Maria Angélica Figueiredo. **Implantação de uma gestão da segurança da informação através da abordagem seis sigma.** 2009. 191 f. Dissertação (Mestrado) - Curso de Engenharia de Produção, Universidade Federal de Santa Maria, 2009. Disponível em: http://cascavel.cpd.ufsm.br/tede/tde_busca/arquivo.php?_cod Arquivo=2531. Acesso em: 13 nov. 2011.

OLTRAMARI, Alexandre. Hora de prestar contas: Antonio Palocci é denunciado ao STF pela quebra ilegal de sigilo do caseiro Francelino. **Veja,** São Paulo, n. 2050, p.54-54, 05 mar. 2008

OSGOOD, Charles Egerton; SUCI, George J.; TANNENBAUM, Percy H. **The measurement of meaning**. Urbana, USA: University of Illinois Press, 1957. 342 p.

PARKER, Donn B. **Fighting computer crime**: a new framework for protecting information. New Jersey: John Wiley & Sons, 1998.

PARKER, Donn B. Security motivation, the mother of all controls, must precede awareness. **Computer Security Journal**, v. 15, n. 4, p. 15-23, 1999.

PARKS, R. C.; DUGGAN, D. P. Principles of Cyber-warfare.In: IEEE WORKSHOP ON INFORMATION ASSURANCE. West Point, NY. **Proceedings... .** West Point, NY: IEEE, 2001. p. 122 - 125.

PATEL, Sandip C.; SANYAL, Pritimoy. Securing SCADA systems. **Journal of Information Management and Computer Security**, v. 16, n. 4, pp. 398-414, 2008.

PELTIER, Thomas R., **Information security risk analysis**. Boca Raton: Auerbach Publications, 2001.

PFLEEGER, Charles P., **Security in Computing.** 2ª. Edition. Editorial Precision Graphic Services Inc. NJ 07458. 1997. USA.

PIPKIN Donald L. **Information security**: protecting the global enterprise. New Jersey, USA: Prentice Hall PTR, 2000.

PRICEWATERHOUSECOOPERS (Org.). **Pesquisa global de segurança da informação,** 2013 Disponível em: <http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-13.pdf>. Acesso em: 03 set. 2013

PUHAKAINEN, Petri. **A design theory for information security awareness.** 2006. 156 f. Tese (Doutorado) - Faculty of Science, Department of Information Processing Science, University of Oulu, Oulu, Finland, 2006. Disponível em: http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf. Acesso em: 17 jan. 2011.

RAMOS, Anderson (org.). **Security Officer 1**: Guia Oficial para Formação de Gestores em Segurança. 2. ed. Porto Alegre: Zouk, 2008.

RAMOS, Isaías de Queiroz. **Contribuição da ciência da informação para a criação de um Plano de Segurança da Informação.** 2007. 117 f. Dissertação (Mestrado) - Programa de Pós-graduação em ciência da informação, Centro de ciências Sociais Aplicadas, Pontifícia Universidade Católica de Campinas, Campinas, 2007.

REINO UNIDO. BERR Department for Business Enterprise & Regulatory Reform. **Information security breaches survey**: Thecnical report. PriceWaterhouseCoopers, 2008.

REINO UNIDO. GAMMA. **The history of ISO/IEC 27001**. Disponível em http://www.gammassl.co.uk/27001/history.php. Acesso em: 13 fev. 2013.

REINO UNIDO. Office of Government Commerce. **ITIL v.3 foundation** – Service Operation. Buckinghamshire, 2011.

REZENDE, Denis Alcides; ABREU, Aline Franca. **Tecnologia da informação aplicada a sistemas de informação empresariais.** 3. ed. São Paulo: Atlas, 2003.

RIBEIRO, John. China tem grupos de ciberespionagem que rouba segredos dos EUA, diz relatório. **IDGNOW!** Disponível em: http://idgnow.uol.com.br/internet/2013/02/19/china-tem-grupo-de-ciberespionagem-que-rouba-segredos-dos-eua-diz-relatorio/. Acesso em: 19 abr. 2013.

SALATIEL, José Renato. Crimes virtuais: hackers promovem onde ataques no Brasil. **Uol - Vestibular**: Resumos das Disciplinas : atualidades**,** São Paulo, p.3-3, 01 jul. 2011. Diário. Disponível em: <http://vestibular.uol.com.br/resumo-das-disciplinas/atualidades/crimes-virtuais-hackers-promovem-onda-de-ataques-no-brasil.htm>. Acesso em: 19 abr. 2013.

SALEH, Mohamed Saad; ALRABIAH, Abdullah; BAKRY Saad Haj. A STOPE model for the investigation of compliance with ISO 17799-2005. **Information Management & Computer Security**, v. 15, n. 4, p.283-294, 2007.

SARACEVIC, Tefko. A ciência da informação: origem, evolução e relações. **Perspectivas em ciência da informação**. Belo Horizonte, v.1, n.1. p. 41-62, jan./jun. 1996.

SARACEVIC, Tefko. Interdisciplinary nature of information science. **Ciência da informação,** Brasília, v. 24, n. 1, 1995. Disponível em: http://revista.ibict.br/ciinf/index.php/ciinf/article/view/530/482. Acesso em: 30 mar. 2010.

SECURITY CONTROLS FOR COMPUTER SYSTEMS (U): Report of Defense Science Board Task Force on Computer Security. Washington: The Rand Corporation, 1970. Disponível em: http://csrc.nist.gov/publications/history/ware70.pdf Acesso em: 26 jun. 2011.

SÊMOLA, Marcos. **Gestão de segurança da informação**: uma visão executiva. 3.ed. Rio de Janeiro: Elsevier, 2003.

SILVA, Abílio Ferreira da; CARVALHO, Mônica Marques; SILVA, Eliane Ferreira da. **Segurança da Informação**: o fator humano. IN: Congresso Brasileiro de Biblioteconomia, Documentação e ciência da informação, 22., 2007, Brasília.

SILVA, Claudete Aurora. **Gestão da Segurança da Informação**: um olhar a partir da ciência da informação. 2009. 99f. Dissertação (Mestrado) - Programa de Pós-graduação em ciência da informação, Centro de ciências Sociais Aplicadas, Pontifícia Universidade Católica de Campinas, Campinas, 2009.

SILVA, Jonathas Luiz Carvalho; FREIRE, Gustavo Henrique de Araújo. Um olhar sobre a origem da ciência da informação: indícios embrionários para sua caracterização identitária. ***Encontros Bibli:*** *revista eletrônica de biblioteconomia e ciência da informação, v. 17, n. 33, p. 1-29, jan./abr., 2012. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2012v17n33p1/21708*

SILVA, Luiz Fernando Costa Pereira da. **Gestão de risco em tecnologia da Informação como fator crítico de sucesso na gestão de Segurança da Informação dos órgãos da Administração Pública Federal:** um estudo de caso da Empresa Brasileira de Correios e Telégrafos – ECT. 2010. 163 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação em ciência da informação, Faculdade de Economia Administração e ciência da informação e Documentação. Departamento de ciência da informação, Universidade de Brasília, Brasília, 2010.

SILVA, Rozelito Félix da. **Proposta de adaptação do modelo Balanced Scorecard (BSC) para a gestão de segurança da informação em órgãos da administração pública**. 2010. 82 f. 2010. xiv, 82 f. : Dissertação (mestrado) - Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, 2010.

SIPONEN, Mikko T. On the role of human morality in information system security: the problems of descriptivism and non-descriptive foundations. IN: Annual Working

Conference on Information Security for Global Information Infrastructures, 15. **Proceedings...** Devender, The Netherlands: IFIP, p. 401-410, 2000.

SMITH, Adam. **A riqueza das nações**. São Paulo: Nova Cultural, 1988. V.1

STAIR, Ralph M.; REYNOLDS, Georges W. **Princípios dos sistemas de informação.** Rio de Janeiro: LTC, 2002.

STANTON, Jeffrey M. *et al*. Behavioral information security: defining the criterion space. IN: Mastrangelo P.M.; Everton W.J. (eds). **The Internet at work or not**: preventing computer deviance. Orlando: Society for Industrial and Organizational Psychology, 2003.

SUMMERS, Rita C. **Secure computing**: threats and safeguards. New York: McGraw-Hill, 1997.

SUPERINTENDENCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO. Universidade Federal do Rio de Janeiro (Ed.). **Incidentes de segurança da informação:** o que é um incidente. 2014. Disponível em: <http://www.tic.ufrj.br/index.php/o-que-sao-incidentes>. Acesso em: 17 jan. 2014.

SYMANTEC. **IT Risk Management Report 2: myths and realities. 2008** Disponível em http://eval.symantec.com/mktginfo/enterprise/other_resources/b-it_risk_management_report_2_01-2008_12818026.en-us.pdf. Acesso em: 27 set. 2011.

TAYLOR, Robert S. **Value-added processes in information systems**. Westport, CT, USA: Greenwood Publishing Group Inc., 1986.

THE SARBANES-OXLEY ACT. In: **Gestão Transparente**. Org: Guia prático de gestão de riscos de corrupção nas organizações. Disponível em: http://gestaotransparente.org/?page_id=146. Acesso em: mar. 2013.

THE WHITE HOUSE. **The National Strategy to Secure Cyberspace:** Appendix Actions and Recommendatios. Washington, 2003. Disponível em: http://www.whitehouse.gov/pcipb/appendix.pdf. Acesso em: 22 jun. 2012.

THE WHITE HOUSE. The National Strategy to Secure Cyberspace: **Priority III**: A National Cyberspace Security Awareness and Training Program. Washington, 2003. Disponível em: http://www.whitehouse.gov/pcipb/priority_3.pdf. Acesso em: 22 jun. 2012.

THOMSON M.E.; VON SOLMS R. An effective information security awareness program for industry. In: Information Security - from Small Systems to Management of Secure Infrastructures. **Proceedings** of the WG 11.2 and WG 11.1 of the TC-11. Copenhagen, Denmark: IFIP, 1997.

THOMSON M.E.; VON SOLMS R. Information security Awareness: educating your users effectively. **Information Management & Computer Security**, v. 6, n. 4, p. 167-173, 1998.

THURSTONE, L. L.; CHAVE, E. J. **The scale - value**. In:___. The measurement of attitude: A psychophysical method and some experiments with a scale for measuring attitude toward the Church. Chicago, University of Chicago, 1929, p. 36-58.

TRIBUNAL DE CONTAS DA UNIÃO. **Resolução nº 217, de 15 de outubro de 2008**. Dispõe sobre a Política Corporativa de Segurança da Informação do Tribunal de Contas da União.

WARE, Willis H.(ed.) **Security controls for computer systems**: Report of Defense Science Board Task Force on Computer Security. Santa Monica, CA: Rand Corporation, 1979.

WASHINGTON: National Institute of Standards and Technology, Building an Information Technology Security Awareness and Training Program, 2003. Disponível em: http://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-50-building-information-security-awareness-program-2003.pdf. Acesso em: 30 nov. 2013.

WELLS, F. Jean; JACKSON, William, D. **Major Financial Services Legislation, The Gramm-Leach-Bliley Act (P.L. 106-102)**: an overview. Washington, The Library of Congress, 1999.

WERSIG, Gernot. Information Science: the study of postmodern Knowledge usage**. Information Processing and Management**, v. 29, n.2, p. 229-239, 1993.

WERSIG, Gernot; NEVELING, Ulrich. The phenomena of Information Science. **The Information Scientist**, v. 9, n. 4. 1975.

WOOD, C.C. The Human Firewall Manifesto. **Computer Security Journal**, v. 18, n.1, p.15-18, 2002.

ZAPATER, Márcio; SUZUKI, Rodrigo. Segurança da Informação – Um diferencial na competitividade das corporações. **Promon Businnes & Technology Review**. Rio de Janeiro, 2005.

ZHANG, Jie. **A model of human factors that affect organizational information security effectiveness.** Mississippi, USA:University of Mississippi, 2006.

ZINS, C. Mapa do conhecimento da ciência da informação: implicações para o futuro da área. **BJIS**, v.1, n.1, p.3-32, jan./jun. 2007. Disponível em: <http://www.bjis.unesp.br/>. Acesso em: 23 nov. 2013.

Apêndice 1 - Questionário valor da informação

QUESTIONÁRIO DE AVALIAÇÃO DO BALANCEAMENTO ENTRE OS PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO – PARTE I

VALOR DA INFORMAÇÃO

Faculdade de ciência da informação

Doutorando: Kelson Côrte

Orientador: Prof. Dr. Rogério Henrique de Araújo Junior

PESQUISA DE CAMPO COMO PARTE DO TRABALHO DE DOUTORADO EM ciência DA INFORMAÇÃO

PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO

QUESTIONÁRIO DE AVALIAÇÃO SOBRE O "VALOR DA INFORMAÇÃO"

Nome da instituição:	
Unidade orgânica:	
Nome do responsável pelo preenchimento do questionário:	
Função:	
E-mail:	
Data:	Telefone:

Instruções para o preenchimento:

1. Indique o quanto você concorda com as afirmações descritas a seguir, assinalando com um "X" no espaço correspondente à resposta que melhor expresse a sua opinião;

2. Todas as questões deverão ser respondidas e, cada delas deverá ter uma única resposta.

Item	Questões/Afirmações	SIM	NÃO
	VALOR DA INFORMAÇÃO	*****	*****
1	O valor da informação é estimado antes de se definir a sua proteção?		
2	Existe uma metodologia definida e estabelecida para se estimar o valor da informação a ser protegida?		
2.1	Se sim, a metodologia existente para a estimativa do valor da informação se apoia em teorias, tais como: valor de uso*, valor de troca*, valor de restrição* ou outra (especificar)?		

Item	Questões/Afirmações	SIM	NÃO
	VALOR DA INFORMAÇÃO	*****	*****
2.2	Se não, existe algum critério para se classificar a informação que leva em consideração questões estratégicas (informação estratégica, tática ou operacional), ou questões de sigilo (ostensivo, confidencial) ou criticidade?		
3	Ao se definir qual a proteção que se dará à informação tem-se o cuidado de calcular o custo da proteção e compará-lo com o valor atribuído à informação, para que o custo da proteção não seja maior do que o valor da informação?		

* Valor de troca: é a troca de dinheiro por produto (informação).

* Valor de uso: é o benefício que uma informação traz ao seu usuário.

* Valor de restrição: está relacionado à informação secreta ou de interesse comercial, quando o uso fica restrito apenas a algumas pessoas.

Comentários:

- Caso o valor da informação não seja estimado de nenhuma das formas indicadas acima, como é estimado o valor da informação?

Apêndice 2 – Questionário pilar pessoas

QUESTIONÁRIO DE AVALIAÇÃO DO BALANCEAMENTO ENTRE OS PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO – PARTE II

PILAR PESSOAS

Faculdade de ciência da informação

Doutorando: Kelson Côrte

Orientador: Prof. Dr. Rogério Henrique de Araújo Junior

PESQUISA DE CAMPO COMO PARTE DO TRABALHO DE DOUTORADO EM ciência DA INFORMAÇÃO

PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO

QUESTIONÁRIO DE AVALIAÇÃO DO PILAR "PESSOAS"

Nome da instituição:	
Unidade orgânica:	
Nome do responsável pelo preenchimento do questionário:	
Função:	
E-mail:	
Data:	Telefone:

Instruções para o preenchimento:

1. Indique o quanto você concorda com as afirmações descritas a seguir, assinalando com um "X" no espaço correspondente à resposta que melhor expresse a sua opinião;

2. Todas as questões deverão ser respondidas e, cada uma delas deverá ter uma única resposta.

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
	PESSOAS	*****	*****	*****	*****	*****	*****	*****
1	A direção superior conhece suas responsabilidades e apoia ativamente a segurança da informação, por meio de claro direcionamento; demonstra seu comprometimento; define atribuições de funcionários, de terceiros e de fornecedores, de forma explicita; cobra e verifica, periodicamente, o cumprimento dessas responsabilidades.							

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
2	A quantidade de pessoal responsável pelos sistemas de segurança da informação é suficiente e está adequada ao porte da empresa e aos riscos a que esta está sujeita.							
3	Os funcionários, os fornecedores e os terceiros conhecem e estão conscientes dos riscos e das ameaças relativas à segurança da informação, que, por essa razão, desenvolvem suas atividades de acordo com a política de segurança da informação, visando reduzir os riscos existentes.							
4	Os funcionários, os fornecedores, os terceiros e os usuários recebem, periodicamente, treinamento apropriado sobre as questões de segurança da informação; permanece conscientes e atualizados sobre a política de segurança da informação e sobre os procedimentos para o exercício de suas funções, inclusive sobre definição e sobre utilização de senhas.							
5	Existe um processo disciplinar formal para qualquer funcionário que tenha violado algum procedimento obrigatório estabelecido na política de segurança da informação.							
6	Os direitos de acesso de qualquer funcionário, fornecedor ou terceiro às informações e aos recursos de processamento da informação são imediatamente retirados, após o encerramento de suas atividades, contratos ou acordos, ou são devidamente ajustados após a mudança de suas atividades.							
7	Existe uma política formalmente implementada sobre “mesa limpa de papéis“, “mídias de armazenamento removíveis“ e “tela limpa“ para os recursos de processamento da informação.							
8	Periodicamente, verifica-se como está o balanceamento entre os pilares pessoas, processos e tecnologia.							

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
9	Quando se identifica deficiência no pilar pessoas, realizam-se investimentos para que esse pilar volte a ter condição relativa compatível com sua importância.							

Comentários:

- Caso queira, comente sobre outros aspectos relevantes do pilar pessoas, de sua instituição, em segurança da informação:

Apêndice 3 – Questionário pilar processos

QUESTIONÁRIO DE AVALIAÇÃO DO BALANCEAMENTO ENTRE OS PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO – PARTE III

PILAR PROCESSOS

Faculdade de ciência da informação

Doutorando: Kelson Côrte

Orientador: Prof. Dr. Rogério Henrique de Araújo Junior

PESQUISA DE CAMPO COMO PARTE DO TRABALHO DE DOUTORADO EM ciência DA INFORMAÇÃO

PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO

QUESTIONÁRIO DE AVALIAÇÃO DO PILAR "PROCESSOS"

Nome da instituição:	
Unidade orgânica:	
Nome do responsável pelo preenchimento do questionário:	
Função:	
E-mail:	
Data:	Telefone:

Instruções para o preenchimento:

1. Indique o quanto você concorda com as afirmações descritas a seguir, assinalando com um "X" no espaço correspondente à resposta que melhor expresse a sua opinião;
2. Todas as questões deverão ser respondidas e, cada uma delas deverá ter uma única resposta.

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
	PROCESSOS	*****	*****	*****	*****	*****	*****	*****
1	Existe um documento da política de segurança da informação aprovado pela direção superior, publicado e comunicado a todos os funcionários e partes externas, revisado periodicamente, visando assegurar a sua continua pertinência, adequação e eficácia.							

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
2	Todos os papéis e as responsabilidades de funcionários, de terceiros, de fornecedores e de usuários sobre a segurança da informação estão claramente definidos em documentos formais e são formalmente comunicados aos interessados.							
3	Os requisitos para preservar a confidencialidade das informações estão formalmente definidos e implementados, através de documentos apropriados a funcionários, a fornecedores, a terceiros e a usuários.							
4	São definidos e utilizados perímetros físicos e lógicos de segurança para proteger as áreas que contêm informações e recursos de processamento da informação e o acesso a essas áreas é devidamente controlado, para assegurar que somente pessoas autorizadas tenham acesso.							
5	Existem procedimentos formais de registro e de cancelamento de usuário, com a participação efetiva dos gestores, para garantir e revogar acessos em todos os sistemas de informação e de serviços, de acordo com os requisitos da política de segurança da informação.							
6	Os eventos de segurança da informação são relatados através de canais apropriados da direção, o mais rapidamente possível.							
7	Estão estabelecidos mecanismos de registro para quantificar e para monitorar os incidentes de segurança da informação por tipo, quantidade e custo, e a informação resultante da análise é usada na identificação de incidentes recorrentes ou de alto impacto.							

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
8	Os eventos que podem causar interrupções aos processos de negócio estão identificados, bem como está calculada a probabilidade de tais interrupções ocorrerem e seus respectivos impactos e as consequências para a segurança da informação.							
9	Existem planos de continuidade de negócios desenvolvidos, implementados e testados, periodicamente, visando garantir a manutenção ou a recuperação das operações e, ainda, assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após as interrupções ou falhas dos processos críticos do negócio.							
10	Verifica-se, periodicamente, como está o balanceamento entre os pilares processos, pessoas e tecnologia.							
11	Quando se identifica deficiência no pilar processos, realizam-se investimentos para que esse pilar volte a ter condição relativa compatível com a sua importância.							

Comentários:

- Comente sobre outros aspectos de processo no quesito segurança da informação:

Apêndice 4 – Questionário pilar tecnologia

QUESTIONÁRIO DE AVALIAÇÃO DO BALANCEAMENTO ENTRE OS PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO – PARTE IV

PILAR TECNOLOGIA

Faculdade de ciência da informação

Doutorando: Kelson Côrte

Orientador: Prof. Dr. Rogério Henrique de Araújo Junior

PESQUISA DE CAMPO COMO PARTE DO TRABALHO DE DOUTORADO EM ciência DA INFORMAÇÃO

PILARES QUE SUSTENTAM A SEGURANÇA DA INFORMAÇÃO

QUESTIONÁRIO DE AVALIAÇÃO DO PILAR "TECNOLOGIA"

Nome da instituição:	
Unidade orgânica:	
Nome do responsável pelo preenchimento do questionário:	
Função:	
E-mail:	
Data:	Telefone:

Instruções para o preenchimento:

1. Indique o quanto você concorda com as afirmações descritas a seguir, assinalando com um "X" no espaço correspondente à resposta que melhor expresse a sua opinião;
2. Todas as questões deverão ser respondidas e, cada uma delas deverá ter uma única resposta.

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
	TECNOLOGIA	*****	*****	*****	*****	*****	*****	*****
1	Todos os ativos da organização estão claramente identificados e existe um inventário estruturado e atualizado, bem como regras formalmente definidas para o uso deles.							

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
2	A quantidade, as configurações e as atualizações dos equipamentos estão adequadas ao volume de processamento de dados e às aplicações de segurança da informação necessárias para se ter a proteção desejada.							
3	Todos os equipamentos que processam dados relevantes estão hospedados em local seguro e protegidos para reduzir os riscos de acesso não autorizado e de acidentes ambientais.							
4	Os recursos de desenvolvimento, de manutenção, de teste, de homologação e de produção são separados para reduzir o risco de acessos ou de modificações não autorizadas aos sistemas em produção e aos sistemas operacionais.							
5	O gerenciamento dos serviços terceirizados possui mecanismos que garantem a implementação, a manutenção e o controle do nível apropriado de segurança da informação para os serviços constantes nos acordos de entrega.							
6	As modificações nos recursos de processamento e os critérios de aceitação para novos sistemas, assim como atualizações ou novas versões são devidamente planejados, estabelecidos e são efetuados testes apropriados de segurança no(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.							
7	Existem mecanismos de controles implementados e atualizados para a detecção, a prevenção, a recuperação e a proteção contra códigos maliciosos.							

Item	Questões/Afirmações	discordo totalmente (0 a 9)	discordo (10 a 29)	discordo parcialmente (30 a 49)	concordo parcialmente (50 a 69)	concordo (70 a 89)	concordo totalmente (90 a 100)	Não se aplica
8	Existe uma política de geração de cópias de segurança de todos os bancos de dados e arquivos relevantes, com critérios bem definidos e a execução dessa cópia é efetuada e testada regularmente.							
9	As redes de comunicação de dados são gerenciadas, controladas e protegidas contra ameaças de acessos não autorizados e os parâmetros de segurança são periodicamente revistos e atualizados.							
10	Os registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação são produzidos e mantidos por um período de tempo suficiente para auxiliar futuras investigações e monitoramento de controle de acesso.							
11	Os requisitos para garantir a confidencialidade, autenticidade e proteger a integridade das informações são identificados, implementados e controlados.							
12	Periodicamente, realiza-se ampla verificação para identificar fragilidades/oportunidades de vazamento de informações e ações são imediatamente adotadas, visando mitigar os riscos identificados.							
13	Verifica-se, periodicamente, como está o balanceamento entre os pilares tecnologia, processos e pessoas.							
14	Quando se identifica deficiência no pilar tecnologia, realizam-se investimentos para que esse pilar volte a ter condição relativa compatível com a sua importância.							

Comentários:

- Comente sobre outros aspectos relevantes do uso da tecnologia no quesito segurança da informação:
- Quantos incidentes de segurança da informação ocorreram em 2012?

Anexo 1 – Fontes para revisão de literatura – pilar pessoas

Estudo	Fonte
Aytes and Connolly (2003)	Proceedings of the Ninth Americas Conference on Information Systems
Banerjee, Cronan and Jones (1998)	MIS Quarterly, Vol. 22, No. 1
Barman (2002)	IS security Policies, New Riders Publishing
Beatson (1991)	Proceedings of the Sixth IFIP International Conference on Computer Security
Bray (2002)	Information system security, Vol. 11, No. 1
Cox, Connolly and Currall (2001)	VINE, Issue 123
Denning (1999)	Information Warfare and Security, ACM Press
Desman (2002)	Building an IS security Awareness Program, Auerbach Publications
Forcht, Pierson and Bauman (1988)	Proceedings of the ACM SIGCPR conference on management of information systems personnel
Furnell, Gennatou and Dowland (2001, 2002)	2nd AISM Workshop, International Journal of Logistics Information Management, Vol. 15, No. 5
Furnell, Sanders and Warren (1997)	Proceedings of Medical Informatics Europe '97
Gaunt (1998)	International Journal of Medical Informatics, Vol. 49, No. 1
Gaunt (2000)	International Journal of Medical Informatics, Vol. 60, No. 2
Hadland (1998)	Proceedings of New Networks, Old Information: UKOLUG98, UKOLUG's 20th Birthday Conference 1998
Hansche (2001a)	Information System Security, Vol. 10, Issue 1

Estudo	Fonte
Hansche (2001b)	Information System Security, Vol. 10, Issue 3
ISF (2005)	International Security Forum (ISF), http://www.isfsecuritystandard.com/index_ie.htm
ISO/IEC standard 17799:2005	International Organization for Standardization (ISO)
Kabay (2002)	Computer Security Handbook, Fourth Edition, John Wiley & Sons
Kajava and Siponen (1997)	Proceedings of IFIP-TC 11, 13th International Conference on IS security: IS security Management - The Future
Katsikas (2000)	International Journal of Medical Informatics, Vol. 60, No. 2
Kluge (1998)	International Journal of Medical Informatics, Vol. 49, Issue 1
Kovacich (1998)	Information system security Officer's Guide: Establishing and Managing an Information Protection Program, Butterworth-Heinemann
Kovacich and Halibozek (2003)	The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program, Butterworth-Heinemann
Lafleur (1992)	Computer Control Quarterly, Vol. 10, No. 4
Markey (1989)	Proceedings of the Fifth IFIP International Conference
Martins and Eloff (2002)	Proceedings of IFIP TC11 17th International Conference on IS Security
McLean (1992)	Proceedings of Eighth International Conference on IS security
Mitnick (2002)	The Art of Deception: Controlling the Human Element of Security, Wiley Publishing

Estudo	Fonte
Murray (1991)	Proceedings of the IFIP TC11 Seventh International Conference on IS security
NIST (1996)	National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
NIST (1998)	National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
NIST (2003)	National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
Parker (1998, 1999)	Computer Security Journal, Vol. 15, No. 4; A new Framework for Protecting Information, John Wiley & Sons, USA.
Peltier (2000, 2002)	Computer Security Journal, Vol. 16, No. 2; IS security Policies, Procedures, and Standards. Guidelines for Effective IS security Management, Auerbach Publications
Perry (1985)	Strategies for Computer Security, Butterworth Publishers
Pipkin (2000)	IS security: Protecting the Global Enterprise, Hewlett-Packard Professional Books, Prentice Hall PTR
Proctor and Byrnes (2002)	The Secured Enterprise: Protecting Your Information Assets, Prentice Hall
Rudolph, Warshawsky and Numkin (2002)	Computer Security Handbook, Fourth Edition, John Wiley & Sons, USA
Sasse, Brostoff and Weirich (2001)	BT technology journal, Vol. 19, No. 3

Estudo	Fonte
Schlienger and Teufel (2002)	Proceedings of IFIP TC11, 17th International Conference on Information Security, Security in the Information Society: Visions and Perspectives
Siponen (2000a)	Information Management & Computer Security, Vol. 8, No. 1
Siponen (2000c)	Proceedings of IS security for Global Information Infrastructures, IFIP TC11 Fifteenth Annual Working Conference on IS security
Spurling (1995)	Information Management & Computer Security, Vol. 3, No. 2
Stacey (1996)	Information System Security, Vol. 5, Issue 2
Straub (1990)	Information Systems Research, Vol. 1, No 3
Straub, Carlson and Jones (1993)	Journal of Management Systems, vol. 5, No. 1
Straub and Welke (1998)	MIS Quarterly, Vol. 22, No. 4
SSE-CMM (1999)	Systems Security Engineering - Capability Maturity Model http://www.sse-cmm.org/model/images/ssecmmv2final.pdf
Telders (1991)	Computer Security Journal, Vol. 7, No. 2
I^2SF (1999)	MIT Information Services and Technology (IST) http://web.mit.edu/security/www/gassp1.html
Thomson and von Solms (1997)	Proceedings of the WG 11.2 and WG 11.1 of the TC11 IFIP
Thomson and von Solms (1998)	Information Management & Computer Security, Vol. 6, No 4
Tudor (2001)	IS security Architecture, An Integrated Approach to Security in the Organization, Auerbach Publications

Estudo	Fonte
Vroom and von Solms (2002)	Proceedings of IFIP TC11 17th International Conference on IS security
Vyskoc and Fibikova (2001)	Proceedings of the IFIP WG 9.6/11.7 Working-Conference
White House (2003a, 2003b)	White House www.whitehouse.gov/pcipb/priority_3.pdf; http://www.whitehouse.gov/pcipb/appendix.pdf
Wood (2002)	Computer Security Journal, Winter 2002, Vol. 18, No. 1
Wood (1995)	Computer Fraud & Security Bulletin, June 1995

Fonte: adaptado de Puhakainen (2006).

Anexo 2 – Matérias na mídia sobre incidentes em segurança da informação

COMPUTERWORLD - O portal voz do mercado de TI e Comunicação

Falta de conhecimento sobre riscos adiam planos de segurança da informação

Para RSA, pequenas empresas estão mais vulneráveis por acreditarem que não são alvo de cibercriminosos.

DÉBORAH OLIVEIRA (*)
27 de fevereiro de 2013 - 13h36

Se você acredita que sua companhia não está na mira de cibercriminosos porque é pequena está enganado. O maior desafio das empresas, hoje, quando o assunto é segurança da informação, é a falta de conhecimento dos riscos. Esse cenário, afirma Rogerio Morais, vice-presidente para América Latina da RSA, faz com que as organizações adiem planos de proteção e fiquem vulneráveis a ataques.

"O risco é muito claro. Os hackers querem informações e dinheiro, mas sem fazer barulho. As pessoas pensam que isso é fantasia e esse é o grande perigo", alerta Morais.

O vice-presidente para América Latina, há cinco meses no cargo, diz que desde que atua na área de segurança da informação, em 1998, escuta que a prioridade das empresas é a proteção do ambiente. Mas a intenção não passa de discurso e é pouco praticada. "O investimento somente acontece de forma reativa quando há perda de dinheiro, especialmente em casos de fraude", relata.

Além disso, prossegue, companhias estão investindo em anti-vírus, firewalls e esquecendo de aplicar controles de acesso, monitorar o que acontece dentro da empresa e ainda conscientizar os funcionários sobre a importância da segurança. "O segredo de uma estratégia bem-sucedida é controlar pessoas e proteger informações e transações", observa.

Ele lembra que o elo mais fraco na cadeia de segurança ainda são as pessoas. "Por isso que treinamentos são necessários", completa. Morais alerta que nenhuma pesquisa de mercado mostra ataques caindo. O interesse por dados das empresas cresce cada vez mais e é preciso contar com ferramentas de controle para responder rapidamente aos incidentes.

Hoje, diz Limor Kessem, especialista em comunicação de cibercrime e fraudes online da RSA, o Brasil é um dos três países na América Latina, ao lado de México, Colômbia e Chile, alvo de ataques. "O Brasil recebeu a maioria, ou 42%, dos ataques em 2012", detalha. Malware e trojans ainda são as armas preferidas usadas pelos criminosos para usuários e empresas desatentas.

O País é ainda a quarta maior nação alvo de ataques de phishing no mundo, depois dos Estados Unidos, Grã-Bretanha e Alemanha. O crescimento acelerado de usuários digitais é uma das razões para o salto.

Limor recomenda que as empresas reforcem seus sistemas de autenticação e fiquem sempre alerta. "Muitos problemas demoram anos para serem descobertos. Quando a empresa chega até ele, milhares de dados foram levados para fora", assinala.

(*) A jornalista viajou a San Francisco, nos Estados Unidos, a convite da RSA

http://computerworld.uol.com.br/seguranca/2013/02/27/falta-de-conhecimento-sobre-riscos-adiam-planos-de-seguranca-da-informacao/

COMPUTERWORLD - O portal voz do mercado de TI e Comunicação

Ataques de phishing causam prejuízo de US$ 1,5 bilhão em 2012

De acordo com RSA, Brasil ficou em quarto lugar entre os países que mais tiveram empresas atacadas no ano passado por esse tipo de golpe.

DA REDAÇÃO
31 de janeiro de 2013 - 18h05

O ano passado foi recorde em ameaças virtuais, afirma relatório da RSA, divisão de segurança da EMC. O "Relatório de Fraudes" de dezembro de 2012 aponta crescimento de 59% no total de ataques de phishing no mundo em comparação com o ano anterior. Segundo o levantamento, esses tipo de fraude eletrônica, caracterizada pela tentativa de adquirir informações sigilosas por meio da web, causou prejuízo de 1,5 bilhão de dólares para a economia mundial, expansão de 22%.

Reino Unido, Estados Unidos, Canadá, Brasil e África do Sul são os países que mais tiveram empresas atacados no ano, respectivamente. O Brasil registrou 5% do volume total de ataques. O País está em quarto lugar entre os principais países hospedeiros de phishers, com 4% dos ataques hospedados, indica o estudo.

Segundo a RSA, em 2012, sites de companhias aéreas e de varejo, bem como plataformas de jogos, provedores de comunicação móvel e serviços de webmail foram os alvos do cibercrime. Lojas de varejo online estavam no topo da lista. Cibercriminosos criaram páginas na web comuns, que imitavam as homepages de varejistas. Assim, conseguiram enganar milhares de usuários e acessar dados pessoais e corporativos.

Para 2013, a RSA prevê que os ataques vão continuar a crescer e especialmente em diferentes partes do mundo. A preocupação agora é o phishing em dispositivos móveis. "Com o crescimento exponencial de aparelhos móveis, cibercriminosos estão se aproveitando desses recursos para criar novas táticas", afirma Marcos Nehme, diretor da Divisão Técnica para a América Latina e Caribe da RSA.

Nehme aponta que os criminosos virtuais devem criar aplicativos falsos e liberá-los para donwload em lojas de apps. Rede sociais também têm sido alvo dos phishers, finaliza.

http://computerworld.uol.com.br/seguranca/2013/01/30/ataques-de-phishing-causam-prejuizo-de-us-1-5-bilhao-em-2012/

IDGNOW!

China tem grupo de ciberespionagem que rouba segredos dos EUA, diz relatório.

John Ribeiro, IDG News Service 19 de fevereiro de 2013 - 16h02

Empresa de segurança identificou o grupo como sendo unidade do Exército Popular de Libertação; Unidade fica em Xangai e invade empresas americanas.

Um novo relatório relacionou um grupo de ameaça cibernética, especificamente uma unidade disfarçada sob o nome "Unit 61398", ao Exército de Libertação Popular da China.

A empresa de segurança Mandiant disse em um relatório liberado nesta terça (19/2) que um grupo que vinha sido investigado, chamado de Ameaça Avançada Persistentes (APT1), é uma organização de ciberespionagem que conta com o apoio do governo chinês.

"Na tentativa de identificar a organização por trás dessa atividade, nossa pesquisa mostrou que a Unidade 61398, do Exército Popular de Libertação (PLA), é semelhante ao APT1 em sua missão, capacidades e recursos", disse a Mandiant em seu relatório. "Essa Unidade se encontra precisamente na mesma área em que as atividades do APT1 parecem se originar".

A Unidade 61398 está localizada em um edifício de 130 mil metros quadrados na rodovia Datong, em Gaoqiaozhen, em Pudong New Area (distrito de Xangai).

A natureza do trabalho da unidade é considerada pela China um segredo de Estado, mas a Mandiant acredita que ela está envolvida em operações maliciosas de redes de computadores.

O grupo tem um histórico suspeito, de acordo com empresa de segurança, que desde 2006 observou o APT1 comprometer 141 companhias distribuídas por 20 grandes indústrias - sendo 87% delas sediadas em países onde o inglês é a língua nativa, e estão em setores que a China identificou como estratégico.

O APT1 utiliza ferramentas que a empresa de segurança identificou não serem utilizadas por outros grupos, incluindo duas ferramentas para roubo de e-mails chamadas GETMAIL e MAPIGET.

Uma vez que o grupo estabeleceu o acesso, periodicamente revisita a rede da vítima durante vários meses ou anos para roubar propriedade intelectual, incluindo projetos de tecnologia, processos de fabricação, resultados de testes, planos de negócios, documentos importantes, acordos de parceria, e-mails e listas de contatos pertencentes aos líderes das organizações-alvo, disse a Mandiant.

O Ministério das Relações Exteriores da China disse nesta terça-feira que o país se opõe firmemente à pirataria, e apoiou a regulamentação para evitar ciberataques. O governo já havia negado as acusações de que hackers chineses atacaram dois grandes jornais dos Estados Unidos.

O país também tem sido vítima de hacking, com a maior parte dos ataques originados dos EUA, disse o porta-voz do ministério Hong Lei, durante uma conferência de imprensa. "Ataques cibernéticos são transnacionais e anônimos. É muito difícil rastrear a origem dos ataques. Eu não sei como esta evidência no relatório é sustentável", acrescentou.

http://idgnow.uol.com.br/internet/2013/02/19/china-tem-grupo-de-ciberespionagem-que-rouba-segredos-dos-eua-diz-relatorio/

Uma em cada cinco empresas já sofreu ataques cibernéticos sérios

:: Da redação*

:: Convergência Digital **:: 05/03/2013**

Uma pesquisa global sobre cibersegurança com mais de 1,5 mil entrevistados revelou que mais de um entre cada cinco já tiveram a empresa para qual trabalham atacada por ameaça avançada persistente. De acordo com o estudo realizado pela associação global de TI Isaca e patrocinado pela Trend Micro, que atua no segmento de segurança para computação em nuvem, 94% dos entrevistados consideram as ameaças como problemas sérios, embora a maioria das empresas ainda empregue tecnologias ineficazes para se proteger.

Ainda assim, mais de 60% dos respondentes da pesquisa dizem estar prontos para reagir a um ataque APT. As principais ferramentas para essas reações, porém, são antivírus e antimalware (95%) e tecnologias de perímetro de rede, como os firewalls (93%). O estudo mostra que controles de segurança para dispositivos móveis, que podem ser bastante eficazes, são usados com muito menos frequência.

O estudo também constatou que:

1) A perda de propriedade intelectual de uma empresa foi citada como um dos maiores riscos com as ameaças (por mais de um quarto dos entrevistados), seguido de perto pela perda de informações de identificação pessoal de clientes ou funcionários;

2) 90% dos entrevistados acreditam que o uso de sites de redes sociais aumenta a probabilidade de sucesso de uma ameaça;

3) 87% acreditam que a política de uso de dispositivos próprios (BYOD), aliado ao enraizamento ou o jailbreak do aparelho, torna mais provável um ataque bem sucedido;

4) Mais de 80% disseram que suas empresas não atualizaram seus contratos de fornecedores para se proteger contra ataques.

* Com informações da Trend Micro.

http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33168&sid=18#.UYv167Xvsic

IDGNOW!

Hackers prometem novo ataque contra Sony, afirma site

GamePro/EUA

06/05/2011 - 11h59 - Atualizada em 06/05/2011 - 12h01

Segundo CNet, grupo hacker planeja invadir servidores da empresa neste fim de semana e divulgar os dados de usuários de suas redes online.

A Sony ainda nem se recuperou da “invasão externa“ que vazou dados de mais de 100 milhões de usuários de suas redes de games e um grupo de hackers planeja já um novo ataque ainda mais sério contra a empresa japonesa neste fim de semana, segundo informações da rede CNet.

Segundo o site, um observador do canal Internet Relay Chat disse que um terceiro grande ataque está planejado para este fim de semana contra a Sony e que as pessoas envolvidas planejam publicar todas ou algumas das informações de usuários que conseguirem retirar dos servidores da companhia.

O possível ataque seria um teste importante para as novas medidas de segurança da Sony. Mas um novo vazamento, ainda mais anunciado como esse, poderia ser devastador para a já cercada marca da empresa.

Conforme publicamos ontem, 5/5, o grupo hacker Anonymous voltou a negar ter qualquer envolvimento com o ataque às redes PSN e Station.com, que continuam fora do ar. No início de abril, o grupo havia declarado guerra contra a fabricante japonesa.
Por meio de seu blog oficial, a Sony havia prometido a volta da rede PS Network ainda nesta semana - o que não aconteceu até o momento.

Entenda o caso

No dia 26/4, a Sony anunciou que uma “invasão externa“ à sua rede online conseguiu ter acesso aos dados pessoais e talvez informações de senhas, histórico de compras e até números cartão de crédito dos mais de 70 milhões de jogadores que utilizam a rede do PlayStation 3.
O caso é tão sério que, segundo um instituto de pesquisas especializado, o prejuízo da Sony com o vazamento desses dados poderia ultrapassar os 24 bilhões de dólares.

No dia seguinte ao anúncio, começaram a surgir relatos de gamers que tiveram problemas com seus cartões de crédito, de acordo com os sites como Ars Technica e VGN 365.

Ambos afirmam ter recebido um grande número de mensagens, via e-mail, comentários e mensagens via Twitter, de leitores usuários da PSN que dizem ter tido problemas com compras ou saques não autorizados. Dias depois do ataque à PSN, a empresa admitiu que também houve vazamento de informações em sua rede SOE, que continha os mesmos tipos de dados sensíveis, incluindo informações sobre cartões de crédito.

(http://idgnow.com.br/seguranca/2011/05/06/hackers-prometem-novo-ataque-contra-sony-afirma-site/)

INFO Online (Revista Exame – Editora Abril)

Bancos perdem R$ 3,1 bi com fraudes eletrônicas

Por Fabiano Candido, de INFO Online

Domingo, 17 de março de 2013 - 10h49

São Paulo – Segundo pesquisa da consultoria Accenture, os dez maiores bancos do Brasil perderam, no ano passado, cerca de 3,1 bilhões com fraudes eletrônicas.

O estudo engloba fraudes por meios eletrônicos, desvios de dinheiro, assaltos em agências e sumiço de dinheiro dentro dos próprios bancos. Contudo, o estudo – publicado na Folha de S.Paulo – revela que os crimes digitais são responsáveis pela maior parte do dinheiro subtraído dos bancos.

Segundo a Accenture, as ações eletrônicas são divididas. Tem os ladrões que estouram os caixas automáticos para pegar o dinheiro em papel, falsificadores que clonam cartões de créditos e débitos e, ainda, crackers que capturam dados de internautas. Esses últimos usam vírus, programas espiões e até páginas falsas para interceptar os dados bancários dos clientes.

No entanto, nos últimos anos, um novo tipo de ataque ganhou força. Criminosos grampeiam os telefones dos clientes e, durantes as chamadas de voz feitas para os call centers dos bancos, eles capturam as informações bancárias. Depois, fazem uma ligação para o banco e usam os dados obtidos pelas gravações ilegais, diz a Accenture, para efetuar os crimes.

Os crimes eletrônicos, diz a empresa, são feitos por quadrilhas especializadas, de dentro e fora do país. Elas contam com especialistas em tecnologia que exploram todas as brechas de segurança, tanto dos bancos quanto dos clientes.

Segurança – Os bancos brasileiros investem uma fortuna em tecnologia. Grande parte do dinheiro vai para o desenvolvimento de sistemas que fortalecem a segurança no meio eletrônico.

No ano passado, os bancos gastaram cerca de 20 bilhões com tecnologia. Cerca de 4 bilhões foram para proteger os bancos das fraudes eletrônicas. Segundo o estudo, a preocupação dos bancos torna o meio digital bastante seguro. Além disso, os investimentos tornam os bancos nacionais tão protegidos quanto os estrangeiros.

Apesar dos problemas de fraudes, as operações eletrônicas na web são seguras se os clientes usarem as tecnologias de proteção repassadas pelos bancos, como os geradores de chaves de acesso (tokens).

Uol – Atualidades

Crimes virtuais: Hackers promovem onda de ataques no Brasil

José Renato Salatiel, Especial para a Página 3 Pedagogia & Comunicação

01/07/2011 08h04

O governo brasileiro foi alvo da maior onda de ataques a sites oficiais na internet de sua história. As ações começaram em 22 de junho e duraram cinco dias. O grupo que assumiu a autoria é o mesmo que promoveu nos últimos dois meses os ataques a sites de empresas multinacionais, da CIA e do FBI nos Estados Unidos.

Direto ao ponto: Ficha-resumo

Os incidentes colocaram o Brasil na mira de uma nova tendência de ataques virtuais, de motivação política. Eles também deixaram o governo em alerta e mostraram o quanto empresas e Estado estão vulneráveis a invasões e roubo de dados sigilosos no país, além de abalarem a confiança dos usuários brasileiros em serviços públicos oferecidos na internet.

Foram atingidos os sites da Presidência da República, do Portal Brasil, da Receita Federal, da Petrobras e dos ministérios do Esporte e da Cultura. A página na internet do Instituto Brasileiro de Geografia e Estatística (IBGE) foi outra "vítima" dos hackers.

Ao todo, 20 portais do governo federal e 200 sites municipais, principalmente de prefeituras, foram afetados, de acordo com estimativa feita pelo Serpro (Serviço Federal de Processamento de Dados).

Na maior parte dos casos, os hackers usaram o método conhecido como DoS (Denial of Service, em português, "negação de serviço"). Ele consiste em infectar milhares de máquinas com programas robôs para que façam acessos simultâneos a determinado site ou serviço na rede. O servidor, que possui um limite de acesso, não consegue responder e trava ou desliga, tirando a página do ar.

Neste tipo de ataque não há invasão do computador ou roubo de dados pessoais. Mas ele pode causar prejuízos a milhares de pessoas que

dependem dos serviços oferecidos on-line. Sites de governos foram tirados do ar por meio dessa técnica. A maioria das investidas partiu de computadores da Itália, para dificultar o rastreamento das autoridades.

Na internet, os autores chegaram a divulgar informações pessoais sobre funcionários da Petrobras, a presidente Dilma Rousseff e do prefeito de São Paulo, Gilberto Kassab. As informações, no entanto, eram falsas ou de conhecimento público.

Já o site do IBGE sofreu um tipo diferente de hackeamento. A homepage (página de abertura) do site foi desfigurada, isto é, foi substituída por outra, contendo a imagem de um olho humano pintado como a bandeira do Brasil e um texto com ameaças de novos ataques. Neste caso, houve invasão, mas, segundo o órgão, nenhum dado foi violado.

Em resposta, o governo informou que realizou a manutenção em alguns portais, para aumentar a segurança. A Polícia Federal abriu uma investigação para tentar identificar e indiciar os responsáveis.

Wikileaks

Os hackers surgiram nos anos 1960 nos Estados Unidos, associados a uma ideologia libertária que pregava o acesso livre a informações na internet. Com o tempo, ficaram mais especializados e surgiram os chamados crackers, criminosos que invadem os computadores para roubar senhas de cartões de crédito e outros dados pessoais dos usuários.

O vandalismo na rede cresceu nos anos 1990. Na década seguinte, foi a vez do aumento dos crimes virtuais. Hoje, há modalidades mais sofisticadas e que envolvem a segurança de países, como a ciberguerra e o ciberterrorismo.

Nos últimos meses se intensificaram as ações políticas na rede contra sites de governos. A explicação é a influência do Wikileaks, site do australiano Julian Assange que ficou famoso ao vazar dados confidenciais de governos na rede (veja indicação de livro abaixo). Assange cumpre prisão domiciliar no Reino Unido enquanto aguarda julgamento por acusações de crimes sexuais.

A autoria dos ataques em massa no Brasil - com exceção do site do IBGE, reivindicada pelo grupo Fail Shell - foi atribuída ao coletivo de hackers

LulzSecBrazil, um braço do Lulz Security (ou LulzSec).

O LulzSec se tornou conhecido em maio deste ano. Em dois meses, o grupo realizou ações contra os sites das empresas de videogame Sony e Nintendo, das redes de televisão americanas Fox e PBS, da CIA (agência de inteligência americana) e do FBI, a polícia federal dos Estados Unidos.

No Reino Unido, o serviço público de saúde NHS também sofreu ataques. Dados de mais de 100 milhões de usuários foram divulgados no Twitter do coletivo. Apenas um suspeito foi preso, o britânico Ryan Cleary, 19 anos, apontado como um dos líderes do grupo. Ele foi libertado após pagar fiança.

Segundo os integrantes, as incursões foram feitas apenas por "diversão". Lulz é uma corruptela da sigla LOLs (Laughing Out Loud ou "rindo alto", uma gíria da internet).

Especialistas classificam o coletivo como "chapéu cinza", que indica danos leves aos alvos, em atos encarados como brincadeiras pelos autores. Os hackers classificados como "chapéus brancos" apenas informam as empresas de suas brechas na segurança, enquanto os "chapéus pretos" ou crackers são considerados criminosos que violam dados sigilosos para obter lucro.

Após 50 dias de atividades, o LulzSec anunciou sua dissolução no dia 26 de junho. Já a variação brasileira do grupo permanece ativa.

Segundo o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), o país registrou 142. 844 incidentes no ano passado. Neste ano, de janeiro a março, foram 90.759. O número corresponde a um aumento em quase 118% em relação ao trimestre anterior e de 220% comparado ao mesmo período em 2010. Os casos incluem invasão de servidores, desfiguração de páginas da web, fraudes, DoS e outros.

Direto ao ponto

O governo brasileiro foi alvo da maior onda de ataques a sites oficiais na internet de sua história. As ações começaram em 22 de junho. Os incidentes mostraram a fragilidade da segurança de serviços públicos na internet e abalaram a confiança dos usuários. Foram atingidos os sites da Presidência

da República, do Portal Brasil, da Receita Federal, da Petrobras, dos ministérios do Esporte e da Cultura e de prefeituras.

Os hackers usaram programas robôs para fazer milhares de acessos simultâneos que tiraram as páginas do ar, num ataque conhecido como DoS (Denial of Service, em português, "negação de serviço"). Neste tipo de ataque não há invasão do computador ou roubo de dados pessoais. Mas ele pode causar prejuízos a milhares de pessoas que dependem dos serviços oferecidos on-line. O coletivo de hackers LulzSecBrazil assumiu a responsabilidade pelos ataques. O grupo é um braço do Lulz Security, que nos últimos dois meses realizou ações contra os sites de empresas e do governo dos Estados Unidos.

Os hackers anunciaram a dissolução do grupo em 26 de junho. A página na internet do Instituto Brasileiro de Geografia e Estatística (IBGE) foi outro alvo dos hackers. A homepage (página de abertura) do site foi modificada pelo grupo Fail Shell. Segundo o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), o país registrou 142. 844 incidentes no ano passado. Neste ano, de janeiro a março, foram 90.759.

José Renato Salatiel, Especial para a Página 3 Pedagogia & Comunicação é jornalista e professor universitário.

(http://vestibular.uol.com.br/resumo-das-disciplinas/atualidades/crimes-virtuais-hackers-promovem-onda-de-ataques-no-brasil.htm)

São Paulo, quarta-feira, 04 de maio de 2011 FOLHA DE S.PAULO mercado

Vazamento pode custar US$ 2 bi à Sony

Dados pessoais de mais de 100 milhões de usuários de PlayStation 3 e do jogo EverQuest são roubados por hackers

Games estão fora do ar, e proteção será revista; sem serviço premium de venda on-line, Brasil fica livre do ataque

CAMILA FUSCO NATÁLIA PAIVA

O roubo de informações pessoais de cerca de 100 milhões de usuários do PlayStation 3 e do jogo on-line EverQuest poderá causar à Sony o maior prejuízo da história entre empresas que passaram por episódios de vazamento de dados de clientes.

*Segundo estimativas da consultoria americana Ponemon Institute, especializada em segurança da informação entre empresas, as perdas são estimadas entre US$* 1,5 bilhão e US$ 2 bilhões.

Até hoje os incidentes mais caros de roubo de dados envolveram 130 milhões de números de cartão de crédito roubados do sistema bancário Heartland Payment System, em 2008, e mais de 100 milhões de contas do varejista americano TJX, entre 2005 e 2006.

Nos dois casos, as perdas máximas atingidas foram de US$ 250 milhões. "O custo da Sony é colossal porque vai da investigação sobre o roubo de dados à modificação dos sistemas de tecnologia necessária a partir de agora, além dos prejuízos à imagem da companhia que lida diretamente com consumo de massa em todo o mundo", afirmou Larry Ponemon, fundador do instituto.

Em 26 de abril a companhia havia informado que dados de 77 milhões de usuários da PlayStation Network, rede de jogos on-line, haviam sido roubados.

Nesta semana, admitiu que outros 25 milhões de vítimas podem estar na lista, que envolve também o sistema Sony Online Entertainment, que tem o jogo EverQuest. Entre as informações extraviadas estão nome, endereço e e-mail das vítimas.

"As pessoas que estavam pensando em comprar um PlayStation 3 provavelmente poderão comprar um aparelho do concorrente em virtude do vazamento dos dados."

(http://www1.folha.uol.com.br/fsp/mercado/me0405201103.htm)