UNIVERSIDADE FEEVALE

DIEGO SAMUEL MARMITT

DESENVOLVIMENTO DE *CHECKLIST* PARA AVERIGUAÇÃO DE SEGURANÇA DA TI EM ÓRGÃOS PÚBLICOS: PREVENÇÃO E CONTORNO DE SINISTROS, E CONTROLE DE ACESSO

(Título Provisório)

Anteprojeto de Trabalho de Conclusão

Novo Hamburgo

2012

DIEGO SAMUEL MARMITT

DESENVOLVIMENTO DE *CHECKLIST* PARA AVERIGUAÇÃO DE SEGURANÇA DA TI EM ÓRGÃOS PÚBLICOS: PREVENÇÃO E CONTORNO DE SINISTROS, E CONTROLE DE ACESSO

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

Orientador: Roberto Scheid

Novo Hamburgo

2012

RESUMO

Cada vez mais as empresas estão dependentes das suas informações, bancos de dados e sistemas. Isso se evidencia pelo uso praticamente obrigatório da informática em todos os setores da sociedade. A informação já virou peça fundamental para os negócios, logrando inclusive vantagem competitiva às organizações. Todavia, como praticamente tudo está interconectado e compartilhado, a informação pode estar vulnerável. É prudente que se tomem medidas para garantir a segurança da informação, seja no acesso lógico aos sistemas, ou físico aos locais onde são armazenadas. Também é motivo de atenção o plano de continuidade e a preservação da informação contra sinistros e incidentes naturais. Há algum tempo essa disciplina está em evidência, colaborando para o avanço da proteção dos sistemas. Entretanto, essa não é uma preocupação generalizada entre as organizações. No setor privado, os departamentos de segurança e as políticas de segurança da informação se fazem mais presentes. Contudo, no ambiente público, prefeituras e demais órgãos não tem dado a devida importância à segurança da Tecnologia da Informação (TI), criando um abismo entre as recomendações e o que é de fato implementado para proteção desse que é um dos principais ativos em qualquer empresa, pública ou privada. A proposta desse trabalho é criar um *checklist* (sistema computacional para coleta, armazenamento e análise dos dados) baseado nas melhores práticas e recomendações de segurança da informação. O intuito é de que esse documento não exerça apenas um papel avaliativo, mas acima de tudo conscientizador, acerca da importância da segurança da informação. Também, será utilizado como um roteiro de pesquisa, a fim de averiguar a aderência momentânea de órgãos públicos da região do Vale do Rio dos Sinos quanto a alguns requisitos de segurança: prevenção e contorno de sinistros, além de controle físico e lógico a ambientes de armazenamento de dados e sistemas de gestão, respectivamente.

Palavras Chave: Segurança em TI. Avaliação de segurança. Órgão público. Gerenciamento de riscos. ABNT NBR ISO/IEC 27002.

SUMÁRIO

MOTIVAÇÃO 4
OBJETIVOS 8
METODOLOGIA 9
CRONOGRAMA 11
BIBLIOGRAFIA 12

MOTIVAÇÃO

Conforme Rehbein (2002), ao longo do tempo a utilização de tecnologia e sistemas de informação, como ferramenta de suporte à execução dos trabalhos, deixou de figurar apenas nas grandes corporações. Empresas de menor porte, bem como o setor público, iniciaram o controle de suas atividades e informações com auxílio da Tecnologia da Informação (TI).

Atualmente, a informação constitui-se como um dos principais ativos nas organizações. Segundo a Associação Brasileira de Normas Técnicas (2005, p. x), a informação pode existir em várias formas: "ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou meios eletrônicos [...]". Outrossim, salienta-se que ela está cada vez mais acessível, seja por meio da Internet, das *Local Area Networks* (LAN's), ou mídias eletrônicas.

Sob a análise de Freitas (2009, p. 8), os inúmeros recursos e a flexibilidade que a tecnologia propicia são atrativos para as pessoas e as empresas. Ambos estão cada vez mais dependentes da própria tecnologia e da informação, pois se tornaram vitais. Tendo em vista esse cenário, é fácil perceber que um requisito importantíssimo é a proteção e segurança da informação. "A informação é um ativo não tangível da organização e assim como os ativos tangíveis e financeiros, a organização deve dedicar sua atenção à segurança deste ativo que [...] possuem" (FREITAS, 2009, p. 8).

De acordo com a Associação Brasileira de Normas Técnicas (2005, p. x), a "segurança da informação é 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". Outra abordagem válida, de Sêmola (2003, p. 43 apud FREITAS, 2009, p. 10), é de que "podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

Por volta de 2006, "o assunto Segurança da Informação tornou-se um dos temas mais importantes dentro das organizações, devido as **fortes necessidades de proteção das informações e grande dependência de TI**" (FERREIRA; ARAÚJO, 2006, p. 17, grifo

nosso). Entretanto, Beal (2008, p. 61 apud FREITAS, 2009, p. 17-18) afirma que a segurança da informação está seguidamente ligada a aspectos negativos, como aumento de custos e perda de desempenho. Para inibir tais fatos, os gestores de TI devem conseguir mensurar e enfatizar o valor agregado da segurança em TI para a organização. Não é tarefa simples, "[...] mas através da análise da classificação da informação e da gestão de riscos será possível demonstrar o quanto se deixou de perder caso algum desastre ocorresse, ou alguma informação confidencial fosse revelada ou mesmo um sistema crítico ficasse fora do ar".

Sob a ótica do *Committee of Sponsoring Organizations of the Treadway Commission*[1] (2007, p. 3), as empresas existem para gerar valor e ao longo de sua vida enfrentam problemas e desafios. "Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor". Ainda de acordo com essa instituição, são os processos de gerenciamento de riscos que auxiliam a gerenciar e tratar as incertezas e os riscos. Nota-se que uma estratégia que alinhe gerenciamento de riscos e vulnerabilidades, com a segurança da informação, pode ser o ponto de equilíbrio para a preservação do próprio negócio e sobrevivência da organização.

Tamanho deve ser o cuidado com a informação e os dados, que a responsabilidade por criar a cultura de preservação e segurança das informações geralmente atribui-se à direção suprema da organização. Para Ferreira e Araújo (2006, p. 23), "[...] é responsabilidade da Alta Administração assegurar que todos os usuários dos sistemas de informação saibam como proteger os ativos da organização (informações, hardware, software etc.) [...]". A gerência deve, portanto, incentivar e homologar a criação de uma política de segurança. Ainda segundo Ferreira e Araújo (2006, p. 11), a recomendação é de que um comitê seja criado para tratar desse assunto. Esse, por sua vez, deveria ser formado por profissionais de vários departamentos, incluindo informática, jurídico, engenharia, recursos humanos, dentre outros, reiterando que a responsabilidade é de toda a organização.

Percebe-se que a segurança da informação pode ser crucial para o adequado andamento dos negócios, seja na gestão pública ou privada. Módulo (2006, p. 8) salienta que a estruturação da área de segurança da informação está avançando nas empresas. Sobre a importância da informação no setor público, Rehbein (2006, p. 14) explica:

---

[1] O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) é uma associação de cinco organizações do setor privado que busca fornecer auxílio à empresas quanto a estratégias de gestão de riscos, controle interno e prevenção de fraudes (COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, 2007).

> O setor público, independentemente da esfera, sofre exigência da sociedade para melhorar sua produção de informações, sob argumento de ampliação da eficiência e transparência. Também conhecido por sua tradição burocrática e organizado segundo uma estrutura funcional estanque, o setor público encontra-se pressionado a adotar modelos gerenciais de administração pautados pelo subsídio da informação para a eficácia da gestão. A informação é, portanto, pré-condição tanto para o funcionamento quanto para o atingimento dos objetivos de uma organização privada ou pública.

Módulo (2006, p. 9) apresenta resultados que mostram apenas 23% dos entrevistados do ramo Governo, com um departamento de segurança estruturado. Consoante com Diniz e Diniz (2009, p. 1), em 2008, a Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União realizou pesquisa que apontou dados preocupantes. "[...] constatou que 64% dos órgãos não possuíam uma Política de Segurança implantada, 80% não classifica suas informações e 75% não fazem análises de riscos". Verifica-se, com isso, que historicamente a preocupação não tem evoluído como deveria. De acordo com os mesmos autores, maior atenção deve ser desprendida por parte da Administração Pública, fundamentando sua afirmação ao dizer que a ausência de uma Política de Segurança da Informação delata a falta de cultura e conhecimento de segurança nos órgãos.

A transparência pública é um assunto em evidência. No entanto, há de se distinguir entre as diferenças do que deve ser realmente publicado, ao que é de caráter sigiloso e tem de ser protegido. A recente Lei da Transparência Pública (Lei Nº 12.527, de 18 de novembro de 2011), também conhecida como Lei de Acesso a Informação, pressupõe acesso à população referente aos investimentos e arrecadação dos entes públicos, por meio da Internet. Diniz e Diniz (2009, p. 21), comentam que, em geral, as informações armazenadas por órgãos públicos são relativas à sociedade. Seriam, portanto, públicas. Mas também "sensíveis". Interpretada pelos mesmos autores, "a CF 1988 em seu art. 5 considera o acesso à informação um direito fundamental, mas o limita perante o devido sigilo" (DINIZ; DINIZ, 2009, p. 21).

> Maior evidência se deu ao tratamento especial da informação nos órgãos públicos após os resultados de auditorias promovidas pelo Tribunal de Contas da União. O Acórdão 1063 (TCU, 2008) cita: A importância do correto tratamento para a confidencialidade, a integridade e a disponibilidade das informações de órgãos públicos é evidente, sem falar na autenticidade, na responsabilidade pelos dados e na garantia de não-repúdio. A própria prestação do serviço de uma instituição pública aos cidadãos depende da confiabilidade das informações por ela tratadas e ofertadas (DINIZ; DINIZ, 2009, p. 22-23).

Diante do que foi exposto acima, surge a questão problemática da presente pesquisa. Qual seja: a ***proposição de um instrumento para averiguar a segurança em órgãos públicos é viável?*** Propõe-se então, a criação de um *checklist* (sistema computacional para coleta, armazenamento e análise dos dados), baseado nas melhores práticas e recomendações de segurança da TI. Não obstante a função de conscientizar sobre a importância da segurança dos

dados, este documento servirá como roteiro de pesquisa, averiguando a aderência de alguns órgãos públicos com relação a determinados requisitos de segurança. Sejam eles: prevenção e contorno de sinistros, controle de acesso lógico a sistemas de gestão e físico a ambientes de armazenamento de dados.

OBJETIVOS

Objetivo geral:

Desenvolver um *checklist* (sistema computacional para coleta, armazenamento e análise dos dados) que possa ser utilizado para verificar quesitos de segurança em TI, envolvendo certos tópicos da tecnologia computacional como prevenção e contorno de sinistros, controle de acesso lógico a sistemas de gestão e físico a ambientes de armazenamento de dados, em dois/três órgãos públicos da região do Vale do Rio dos Sinos, no Rio Grande do Sul.

Objetivos específicos:

O escopo do presente estudo delimita-se pela resolução dos seguintes objetivos específicos, meios pelos quais se buscará resolver a problemática apresentada:

- Examinar e expor o embasamento teórico sobre a segurança de TI;
- Estabelecer parâmetros (métricas) para avaliar a condição de segurança, atrelados aos temas propostos;
- Estruturar o *checklist* para averiguar a segurança de TI em órgãos públicos;
- Analisar, através de *benchmarking*, a existência de alguma ferramenta que avalie a segurança de determinada empresa quanto aos processos de TI;
- Desenvolver uma ferramenta (sistema) para coleta e armazenamento das respostas do *checklist*;
- Verificar a viabilidade do *checklist* mediante levantamento e análise de informações em dois/três órgãos públicos da região do Vale do Rio dos Sinos.

METODOLOGIA

A Figura 1 representa resumidamente a qualificação metodológica da pesquisa a ser empregada nesse trabalho. As caixas escuras representam as abordagens que serão utilizadas, em detrimento das demais (claras).

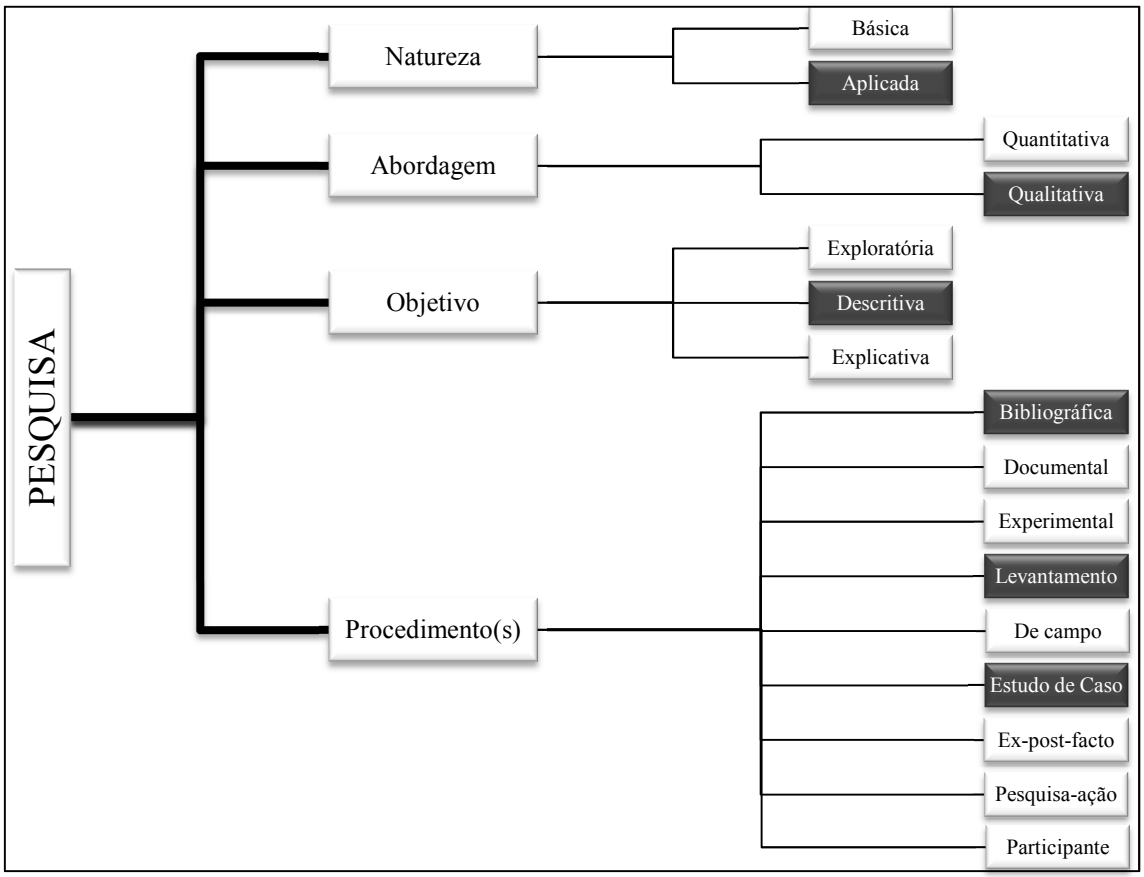

Figura 1 - Classificação da pesquisa
Fonte: adaptada de BEZ (2011, p. 34)

Quanto à natureza, o presente trabalho caracteriza-se como uma pesquisa aplicada, uma vez que se pretende utilizar concepções já definidas e melhores práticas da segurança em TI. Não se almeja criar novos conceitos ou redefinir padrões, mas sim estabelecer um enfoque pontual quanto ao tema em questão, aplicado sob a ótica da área pública.

Essa pesquisa pode ser considerada, também, como qualitativa, referindo a sua abordagem. O resultado almejado, bem como sua análise, não se dará por averiguação estatística, mas sim por coerência e homologação da proposta perante a pesquisa a ser realizada com as organizações públicas.

Como dito anteriormente, o objetivo desse trabalho visa estabelecer um conjunto de fatores (quesitos) a serem utilizados na análise da segurança em TI. O *checklist*, produto final contido desses pontos a serem observados, será validado mediante um levantamento executado junto a alguns entrevistados. No que concerne aos objetivos da investigação, pode-se afirmar que essa é uma pesquisa descritiva, pois buscará levantar fatos para posteriormente analisá-los, sem manipulação do pesquisador.

Os procedimentos a serem realizados para conclusão do presente trabalho qualificam-no de 3 (três) formas:

a) pesquisa bibliográfica: inicialmente será executada uma pesquisa na literatura, com o objetivo de agregar conhecimento e enfatizar as peculiaridades da área em estudo. Conforme Prodanov e Freitas (2009, p. 68), "[...] todas as pesquisas necessitam de um referencial teórico". Portanto, é extremamente prudente uma análise inicial ampla sobre o assunto, já que essa será fato gerador do produto final desse trabalho;
b) levantamento: modelo mais tradicional de pesquisa. Será aplicado para a coleta de informações que, ao final, sustentarão a análise sobre o tema, assim como servirão para validar, ou não, o emprego do *checklist* proposto;
c) estudo de caso: essa forma de pesquisa também pode ser considerada válida para o trabalho em questão. Prodanov e Freitas (2009, p. 74) destacam que este método "[...] envolve o estudo profundo e exaustivo de um ou poucos objetos de maneira que permita o seu amplo e detalhado conhecimento". Como é desejável conhecer e verificar os níveis de segurança em alguns órgãos públicos, o seu estudo, avulso e particular, justifica a adoção dessa técnica.

CRONOGRAMA

Trabalho de Conclusão I

Etapa	Meses			
	Ago	Set	Out	Nov
Pesquisa bibliográfica acerca dos principais tópicos em segurança da TI.	•	•		
Estudo de trabalhos correlatos sobre segurança da TI em órgãos públicos.	•	•		
Redação do anteprojeto.	•	•		
Revisão do anteprojeto.		•		
Entrega do anteprojeto.		•		
Estudo e aprofundamento das recomendações, normas e melhores práticas em segurança da TI.		•	•	•
Redação do TCC I.		•	•	•
Revisão do TCC I.			•	•
Entrega do TCC I.				•

Quadro 1 – Cronograma previsto para execução do Trabalho de Conclusão I
Fonte: elaborado pelo autor

Trabalho de Conclusão II

Etapa	Meses			
	Mar	Abr	Mai	Jun
Desenvolvimento do sistema para coleta e armazenamento das respostas do *checklist*.	•	•		
Pesquisa de campo sobre aderência de órgãos públicos às recomendações do *checklist* proposto.		•		
Análise e avaliação dos resultados.		•	•	
Redação do TCC II.		•	•	•
Revisão do TCC II.			•	•
Entrega do TCC II.				•
Apresentação dos resultados à banca avaliadora.				•

Quadro 2 – Cronograma previsto para execução do Trabalho de Conclusão II
Fonte: elaborado pelo autor

BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: tecnologia de informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p. Disponível em: <http://www.abntcolecao.com.br>. Acesso em: 10 ago. 2012.

BEZ, Marta Rosecler. **O uso de tecnologia para apoiar a implantação de métodos ativos nos currículos de medicina**. 2011. 117 p. Proposta de Tese (Doutorado em Informática na Educação) – Programa de Pós-graduação em Informática na Educação, Centro Interdisciplinar de Novas Tecnologias na Educação, Universidade Federal do Rio Grande do Sul, UFRGS, Porto Alegre, 2011.

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 União**, Poder Legislativo, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.in.gov.br/visualiza/index.jsp?data=18/11/2011&jornal=1000&pagina=1&totalArquivos=12>. Acesso em: 03 set. 2012.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 2. ed. Brasília, DF: Tribunal de Contas da União, 2007. 70 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 02 set. 2012.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Gerenciamento de riscos corporativos**: estrutura integrada. [S.l.], 2007. 135 p.

DINIZ, Flávio Luiz Ribeiro; DINIZ, Priscila Escórcio de França. **Avaliação preliminar da gestão de segurança da informação em duas organizações públicas**. 2009. 89 p. Monografia (Curso de Computação – Licenciatura), Universidade de Brasília, Brasília, DF, 2009. Disponível em: <http://monografias.cic.unb.br/dspace/bitstream/123456789/235/1/projeto_final_flavio_priscila.pdf>. Acesso em: 05 set. 2012.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu de. **Política de Segurança da Informação**: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006. 177 p.

FONTES, Edison Luiz Gonçalves. **Políticas e normas para a segurança da informação**: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012. 269 p.

FREITAS, Eduardo Antônio Mello. **Gestão de riscos aplicada a sistemas de informação**: segurança estratégica da informação. 2009. 71 p. Monografia, Curso de Pós-graduação "Lato Sensu" em Gestão Estratégica e Qualidade, Universidade Cândido Mendes, Brasília, DF, 2009. Disponível em: <http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/3564/gestao_riscos_freitas.pdf?sequence=4>. Acesso em: 05 set. 2012.

INFOSEC COUNCIL. **Planejamento estratégico da segurança da informação.** São Paulo, 2010. 50 p. Disponível em: <http://www.infoseccouncil.org.br/publicacoes/201001_whitePaper_PlanejamentoPT.pdf>. Acesso em: 27 ago. 2012.

MÓDULO. **10ª pesquisa nacional de segurança da informação**. Rio de Janeiro, 2006. 18 p. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>. Acesso em: 04 set. 2012.

MORAZ, Eduardo. **Treinamento profissional anti-hacker**. São Paulo: Digerati Books, 2006. 128 p.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. Novo Hamburgo: Feevale, 2009. 288 p.

REHBEIN, Airton Roberto. **Avaliação de sistemas de informação**: estudo do sistema de administração tributária da Prefeitura Municipal de Canoas/RS. 2002. 159 p. Dissertação (Mestrado Profissional em Controladoria) – Programa de Pós-graduação em Economia, Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2002. Disponível em: <http://www.lume.ufrgs.br/handle/10183/4200>. Acesso em: 04 set. 2012.

VERAS, Manoel. **Datacenter**: componente central de infraestrutura de TI. Rio de Janeiro: Brasport, 2009. 347 p.