IT OUTSOURCING SERVICES: SECURITY ISSUES

Regivaldo Gomes Costa (Universidade Católica de Brasília, DF, Brasil) - regivaldo.costa@camara.gov.br

Henrique Andrade de Almeida (Universidade Católica de Brasília, DF, Brasil) - henrique.almeida@gmail.com

The process of services outsourcing in Brazil has come of long date. In the area of Information Technology (IT), the decade of 1990 was the great propeller, mainly in the segment of Public Administration. Nowadays, the outsourcing of IT services, for some operational segments, occupies already in 100% the work ranks. The problem, as a whole, elapses of that sensible areas of IT, such as the administration and control of data base, mechanisms of access control, among others, have been outsourcing object. This action can bring serious risks to the institution business in which it refers to the guarantee of the pillars of the Information Security, that is, confidentiality, integrity and availability of the information. The intention of this article is to present some relative references to the Information Security, aiming to the mitigation of risks associated to the processes of outsourcing in sensible areas of IT, having as focus to give visibility, to the public manager, of the risks involved for the business. A set of good practices based on norms, standards and control, is presented as a form of mitigation.

Keywords: IT outsourcing, Risk Management, Information Security, Confidentiality, Integrity

1. Introdução

A legislação brasileira, por meio dos decretos 200/67 e 2.271/97 (que explicitam a informática como área objeto de terceirização), regulamenta que a administração pública procurará desobrigar-se da realização material de tarefas executivas, recorrendo, sempre que possível, à execução indireta, devendo incumbir-se somente das tarefas de planejamento, coordenação, supervisão e controle.

Foi na década de 1990 que o processo de terceirização (também conhecido como *Business Process Outsourcing*, ou simplesmente *outsourcing*) na área de Tecnologia da Informação (TI) efetivamente deslanchou-se de forma surpreendente [PRADO, 2000] em todo o mundo. Nessa época, os serviços dentro da TI, objeto de terceirização, limitavam-se aos serviços operacionais, tais como digitação, manutenção de *hardware*, atendimento ao usuário final e apoio técnico-operacional na infraestrutura e no desenvolvimento de *software*.

Na década de 2000, o processo de terceirização, que já se encontrava em franca expansão, veio à terceirização dos serviços de administração, supervisão e controle em banco de dados, redes e dos mecanismos de segurança. Assim, postos de trabalho, que incluem atividades de planejamento, supervisão e controle, porém em menor escala, passaram a ser objeto de terceirização, contrariando, portanto, o decreto 200/67.

Não é o foco deste trabalho, mas vale ressaltar, na iniciativa privada, a terceirização tem como objetivo redução de custos, minimização da gestão de recursos humanos, melhoria na prestação de serviços, flexibilidade na relação demanda e objeto de contratação, acesso a conhecimentos técnicos e inovações tecnológicas, entre outros de menor relevância.

Já na Administração Pública, o processo de terceirização, sustentado pelos decretos supracitados, é licito, necessário e agrega os benefícios elencados para a iniciativa privada. Porém, o *déficit* de um corpo técnico qualificado, associado às dificuldades legais para contratar por meio de concurso público, são os pontos que mais contribuem no aumento, e muitas vezes indiscriminadamente, da terceirização de TI.

Já há algum tempo que a TI deixou de ser um mero suporte às atividades-meio e passou a ser um componente estratégico dentro das organizações, onde o seu desempenho e o alinhamento estratégico estão diretamente ligados ao sucesso do negócio.

Nesse contexto, terceirizar áreas sensíveis, cujo posto de trabalho implica na manipulação de informação estratégica para o negócio, poderá gerar impactos negativos para a organização, caso o sigilo, a confidencialidade e a integridade da informação venham a ser comprometidas [ABREU, 2009; SCHNEIER, 2002]. Abaixo são listados alguns segmentos da TI, que, se terceirizados, poderão deixar a organização sob ameaça:

a) Administração de banco de dados que armazenam informações referentes a sistemas de folha de pagamento, do mercado financeiro, de benefícios e programas sociais, e de diversos outros considerados como sistemas de missão crítica;

b) Administração do controle de acesso aos recursos computacionais, de usuários e senhas e dos sistemas de segurança como um todo (*firewalls*, IDS, IPS etc.);

c) Desenvolvimento e testes de *software* usados em sistema categorizados na alínea "a".

Em pesquisa realizada por Oliveira *et al*. [2006], na qual participaram 14 empresas públicas da área tributária e com aplicação de questionário contendo 19 questões (Figura 1) relacionadas aos riscos envolvidos no processo de terceirização da TI, os gerentes de nível estratégico e tático dessas organizações mensuraram respectivamente em 7,25 e 8,67 pontos, os riscos relativos à Segurança da Informação, tendo como ênfase o sigilo das informações. Essa pontuação foi a maior entre as 19 proferidas. E teve como base a escala de Likert[1] (de 0 a 9), que permite mensurar a importância da perda potencial decorrente de um resultado indesejável, assim como calcular a probabilidade de ocorrer um resultado negativo. A probabilidade de cada resultado indesejável é avaliada identificando-se e mensurando-se os fatores que influenciam esses resultados (AUBERT *et al*., 1998).

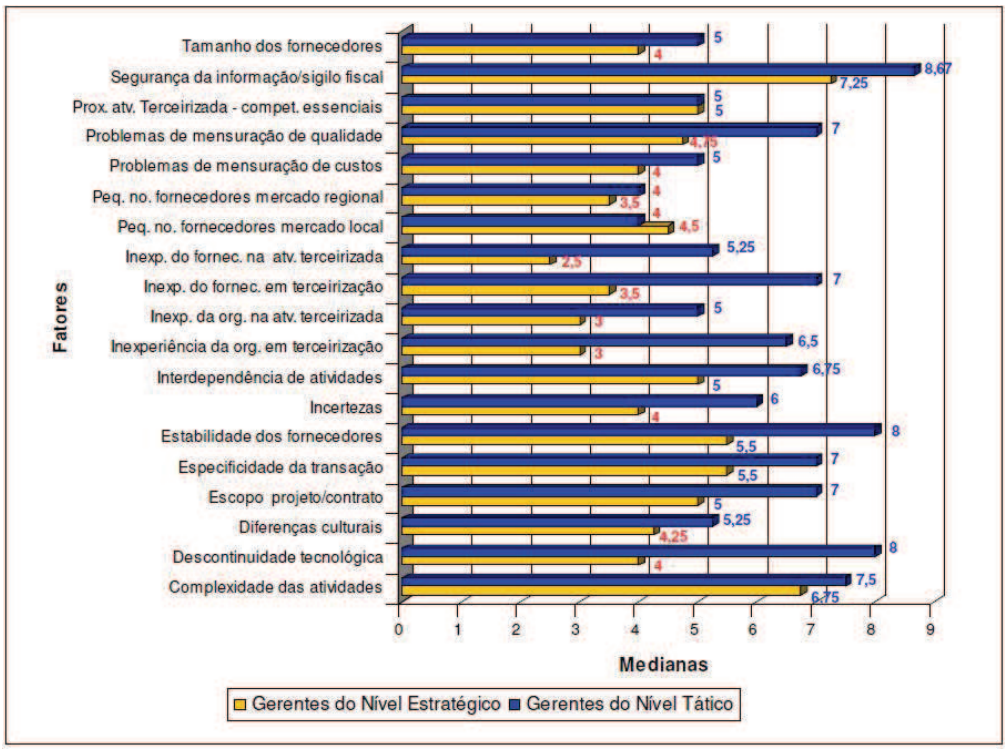

Figura 1: Questões e resultados da pesquisa [OLIVEIRA, 2006]

[1] "A Escala Likert é um tipo de escala de resposta psicométrica usada comumente em questionários, e é a escala mais usada em pesquisas de opinião. Ao responderem a um questionário baseado nesta escala, os perguntados especificam seu nível de concordância com uma afirmação. Esta escala tem seu nome devido à publicação de um relatório explicando seu uso por Rensis Likert".

Esse mesmo estudo revelou que as organizações investigadas utilizam largamente a terceirização em funções de TI, tanto operacionais quanto estratégicas, confirmando ações contrárias aos decretos 200/67 e 2.271/97 na Administração Pública.

Diante do exposto, este trabalho apresenta um conjunto de melhores práticas e o uso do controle para a mitigação dos riscos de segurança envolvidos em áreas de TI de relevância para o negócio [CORDON, 2007], como também, para a geração de subsídios para ações quanto à gestão do processo de terceirização dos serviços de TI. Foge do escopo deste, a apresentação de quaisquer estáticas com base em pesquisas de mercado. Como base estruturante deste trabalho, serão usadas a legislação, normas e padrões internacionais abaixo listadas:

- Normas e padrões Internacionais, tais como “ABNT NBR ISO/IEC” (15408, 7498, 27001:2006, 27002:2005, 27005, 30001), AS/NZ4360, entre outras;
- CobiT (Control Objectives for Information and related Technology);
- Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation);
- Leis e Normas reguladoras.

Este trabalho encontra-se organizado da seguinte forma:

A Seção 1 traz uma introdução do trabalho a ser apresentado;

A Seção 2 apresenta o referencial teórico e trabalhos relacionados quanto à Gestão de Riscos, Segurança da Informação e do processo de terceirização de serviços;

A Seção 3 aborda a metodologia utilizada neste trabalho;

Na Seção 4, foco deste trabalho, serão abordados os problemas e contramedidas (ou boas práticas), conforme proposta;

A Seção 5 traz uma conclusão do que foi apresentado; e

A Seção 6 lista as referências bibliográficas que subsidiaram o trabalho.

2. Referencial Teórico e Trabalhos Relacionados

Com o objetivo de fundamentar este trabalho, possibilitando ao leitor um melhor entendimento do assunto tratado, o que se segue é um referencial teórico de segurança computacional clássica e alguns trabalhos relacionados que abordam a gestão de riscos em processos de terceirização no segmento da Tecnologia da Informação.

2.1 Segurança da Informação

Segundo a norma ISO 27001 [2006], Segurança da Informação (SI) pode ser definida como um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes **integridade**, **confidencialidade**, **autenticidade**, **disponibilidade** e **não-repúdio** (**irretratabilidade**). Esses cinco pilares ou propriedades da SI podem se resumir da seguinte forma:

- **Integridade**: a informação não pode ser passível de alteração por sujeitos não autorizados, seja de forma maliciosa ou acidental;
- **Confidencialidade**: a informação somente poderá ser revelada ao sujeito que detém a autorização sobre a mesma;
- **Autenticidade**: provê garantia da legitimidade de uma identidade;
- **Disponibilidade**: a informação deve estar disponível, a qualquer momento, a sujeitos que são usuários legítimos da mesma;
- **Não-repúdio (irretratabilidade)**: uma comunicação legítima entre duas entidades não pode ser negada por nenhum dos sujeitos que dela participaram.

Dentre essas propriedades, para a segurança dos dados, deve-se focar no que se refere ao nível de proteção, a fim de se prevenir o acesso não autorizado e sua adulteração.

Em Santin [2004], o autor define que segurança em sistemas computacionais não se trata exclusivamente de um meio para permear fins, mas é, antes de tudo, uma disciplina que, por meio de seus conceitos, metodologias e técnicas, tenta manter as propriedades de um sistema, evitando ações danosas de entidades não autorizadas sobre as informações e os recursos do mesmo.

Quando o sistema entra em operação, seja por ser novo ou por ter sofrido modificações, o mesmo pode estar sob ameaça, que compreende procedimentos de exploração de falhas até então desconhecidas. A ação resultante da exploração de falhas é o ataque. Quando se tem uma falha conhecida, pode-se dizer que o sistema está vulnerável.

Pode-se afirmar que os sistemas computacionais estão sempre sujeitos a ameaças e, portanto, passíveis de ataques dos mais variados tipos, os quais decorrem da presença de vulnerabilidades (falhas de programação, configuração, projeto, atualização, entre outras).

2.2 *Framework* para Controle e Segurança de Terceirização em TI

Visando formatar um conjunto de diretivas no que tange à Segurança da Informação (SI) e que permeia o processo de terceirização em TI, Fink [1994] apresenta um *framework* definindo um conjunto de objetivos de controle para TI que proporciona ao gestor ou contratante balizarem melhor sua estratégia de

mitigação/redução de riscos frente a um processo de contratação de fornecedores de serviços de TI.

Fink [1994] defende que há uma quebra de paradigma da SI clássica quando um processo de terceirização é inserido na organização, visto que os ativos tecnológicos e os sistemas de informação são desenvolvidos e operacionalizados pelo fornecedor, havendo, assim, uma perda de controle do gestor sobre os seus ativos e dados. Ainda há um grande risco no que tange à continuidade de negócio, pois, se, por algum motivo, o fornecedor deixar de prestar os serviços, o cliente tem que garantir a fluidez de seus processos de TI com a segurança necessária. Assim, o *framework* proposto se dispõe a suportar esse novo paradigma da SI, tendo como suporte os processos de segurança clássica.

A Figura 2 apresenta uma visão esquemática do quadro de segurança e controle do *framework* composto pelos componentes:

- **Business Recovery**: Identifica as ameaças e elabora contramedidas e procedimentos tendo como meta evitar a ocorrência de desastres;

- **Data Entry, Output and Information Access**: Trata do controle e do acesso aos dados em sistemas de informação, seja de forma local ou distribuída;

- **Organization and Management**: Apresenta diretivas de organização e gerenciamento contribuindo no processo decisório de que áreas devam ser terceirizadas, do controle de qualidade dos serviços, avaliação de parâmetros de confiabilidade e da gerência dos processos de SI e do alinhamento da TI com o negócio;

- **Performance Management**: Este componente tem como objetivo averiguar se o acordo negociado está sendo satisfatório, com base na distribuição de funções ou serviços em um determinado espaço de tempo, que inclui a monitoração de tempo de resposta, capacidade, disponibilidade, métodos de acesso, segurança dos dados, privacidade e autorização de usuários nos sistemas de TI, mas sempre numa perspectiva de segurança e controle;

- **Application Development**: Fomenta o envolvimento conjunto de cliente e fornecedor de serviços em comitês e projetos no planejamento, desenvolvimento, implementação e testes de novos aplicativos ou de alterações aos já existentes, com o objetivo de dirimir conflitos existentes entre as partes.

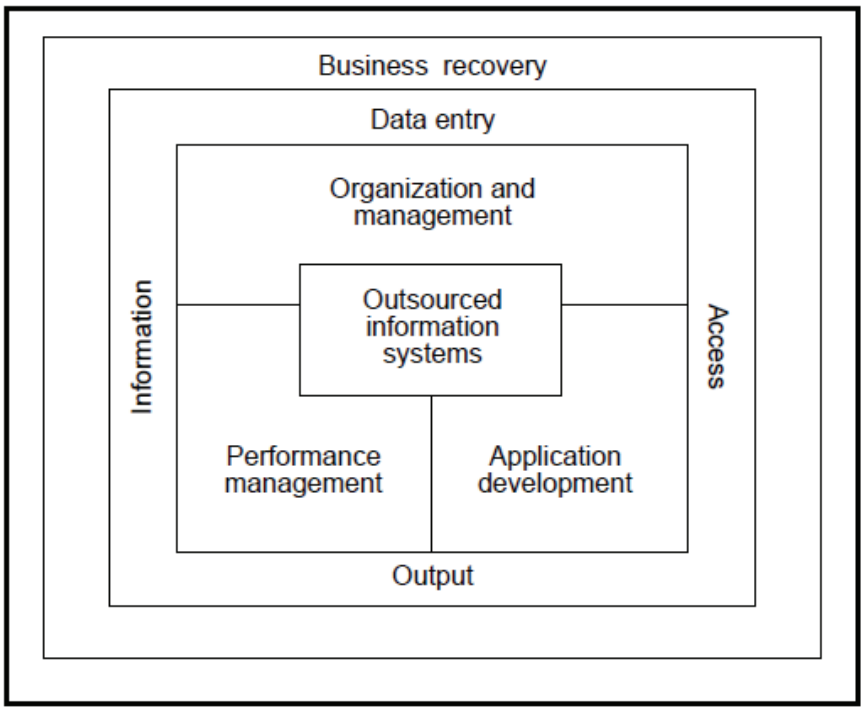

Figura 2: *Framework* para Controle e Segurança de Terceirização em TI (FINK, 1994]

2.3 Estratégias de Segurança Colaborativa em um Sistema Web de terceirizado

Kadakia [2001] afirma que o desenvolvimento de sistemas de TI vem sendo terceirizado de forma abrupta e indiscriminada, gerando novos desafios e motivando a criação de um quadro de gestão de segurança que atenda às normas, regulações e políticas de controle do governo dos Estados Unidos.

Em face desses desafios, o autor apresenta diferentes *frameworks* e discute como integrar diversas metodologias para criar uma completa e abrangente gestão de SI que atenda as necessidades dos processos de terceirização da TI.

O trabalho se baseia em duas metodologias de Certificação e Acreditação (Certification and Accreditation – C & A), que são: NIACAP (National Information Assurance Certification and Accreditation Process) [NIACAP, 2000] e o FIPS 102 (Guideline for Computer Security Certification and Accreditation) [NIST, 1983].

Para a gerência e análise de riscos, o autor se baseia em três *frameworks*. São eles: Information Security Assessment Methodology (IAM/National Security Agency) [IAM, 2001]; do Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE/Carnegie Mellon University's Software Engineering Institute) [ALBERTS *et al.*, 2001]; e do Information Technology Security Assessment Framework (do National Institute of Standards and Technology - NIST) [SWANSON, 2000].

Basicamente, o autor desenvolve um *framework* para avaliação de riscos que compreende um quadro com cinco princípios para análise de riscos abaixo descritos:

- O **primeiro princípio** tem como objetivo avaliar o risco e determinar as necessidades. Contempla também a classificação dos recursos críticos e sensíveis, autorizações, o estabelecimento de controles físicos e lógicos, controle de acesso, investigação de violações e medidas a serem tomadas, gerando, assim, estratégias de proteção que podem ajudar significativamente na gestão dos riscos;

- O **segundo princípio** é de estabelecer um foco central de gerenciamento. Segundo o autor, é um processo importante em terceirização em que a responsabilidade pela segurança nunca pode ser terceirizada e isso cria um importante papel para a gestão e a criação de uma linha de base na relação de confiança. Um número maior de fornecedores e parceiros ganham responsabilidades de segurança, de modo a se tornar importante a necessidade de estabelecer uma base de confiança específica entre as partes;

- O **terceiro princípio** é a implementação de políticas apropriadas e controles relacionados. Deve ser estabelecido um conjunto de políticas obrigatório para uma gestão eficaz do programa de segurança;

- O **quarto princípio** é promover a conscientização. Compreende o envolvimento dos principais dirigentes e dos técnicos. Permite apresentar o porquê dos requisitos de segurança, dos controles de segurança e dos procedimentos de teste associados, da documentação/política que garante e demonstra que os controles de segurança apropriados sejam executados conforme escritos/ determinados. Este é um papel fundamental que a área de SI deve desempenhar e é fundamental para a manutenção efetiva de sistemas seguros;

- O **quinto princípio** é o de monitorar e avaliar a política e a eficácia dos controles. É um processo que deve ser contemplado em tempo integral e possui uma posição de apoio à gestão nos processos de avaliação; protocolos de auditoria; acordos de segurança com fornecedores; integração e implicações na SI; novas melhorias e as implicações de SI; e o processo de Certificação e Acreditação.

O autor finaliza dizendo que a SI depende da capacidade de implementar uma política de segurança que forneça disponibilidade, integridade, autenticação, autorização, privacidade e não-repúdio e que o sistema de gestão de segurança deve ser bem planejado e suas normas devem ser determinadas tão completas quanto possível, antes do desenvolvimento.

Ainda, no governo dos Estados Unidos, as normas, regulamentações e orientações emitidas pela OMB, NIST e GAO podem ajudar a definir metodologias sólidas para a criação de uma metodologia eficaz de certificação e acreditação que leve em conta os desafios de terceirização no governo.

3. Metodologia

A presente pesquisa é de natureza descritiva e referencial, balizando-se em documentos de normas e padrões internacionais, legislação e melhores práticas visando apresentar aos gestores, pontos de referência para a mitigação de riscos em processos de terceirização em TI no tocante a Segurança da Informação (SI); portanto, não é escopo deste trabalho qualquer avaliação qualitativa ou estatística.

O estudo concentrou-se em documentos com foco em SI clássica, gestão de riscos e outros que relacionam a terceirização em TI e SI. O que se segue é uma breve descrição dos principais documentos.

3.1 Norma ABNT NBR ISO/IEC 27001:2006

É uma norma brasileira que promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o Sistema de Gestão de Segurança da Informação (SGSI) de uma organização e adota o modelo conhecido como Plan-Do-Check-Act (PDCA), que é aplicado para estruturar todos os processos do SGSI. Dentro do contexto da SI, ela possibilita que seus usuários tenham os seguintes entendimentos:

- Dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;
- Implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização; monitoração e análise crítica do desempenho e eficácia do SGSI;
- Melhoria contínua baseada em medições objetivas.

3.2 Norma ABNT NBR ISO/IEC 27002:2006

É uma norma que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de SI em uma organização.

Em resumo, é um guia ou código de práticas para desenvolver os procedimentos de segurança da informação em uma organização. Os objetivos de controle apresentados têm como finalidade serem implementados para atender aos requisitos identificados por meio de análise/avaliação de riscos.

A norma contempla 11 seções de controle de SI, totalizando 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos. As 11 seções são: Política de SI; Organizando a SI; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gestão de Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação; Gestão de Continuidade de Negócios; e Conformidade.

3.3 Norma ABNT NBR ISO/IEC 27005:2008, ISO/IEC 31000 e AS/NZ4360

Essas normas fornecem as diretrizes para o processo de Gestão de Riscos de Segurança da Informação e vêm facilitar a implementação da SI tendo como base a gestão de riscos. Aplicam-se a todos os tipos de organização que desejam gerir os riscos que possam comprometer a SI da organização. As normas ISO vêm prover uma clara sustentação à norma 27001:2006.

As normas ISO 27005 e A/NZ4360 adotam o modelo PDCA (Plan, Do, Check, Act), cujo ciclo compreende as seguintes atividades: definição do contexto, análise/avaliação de riscos (identificação, estimativa e avaliação), tratamento do risco, monitoração e análise critica do risco, comunicação do risco e aceitação do risco. A realimentação da cadeia PDCA se dá em todos os demais itens após o bloco análise/avaliação de riscos.

Vale ressaltar que os processos PDCA da norma escrita pela Austrália/Nova Zelândia (AS/NZ4360) diferem da norma ISO apenas pela inexistência do processo “aceitação do risco”.

A ISO/IEC 30001, que visa padronizar as terminologias e os conceitos da gestão de riscos, não concorre com a 27005 e sim, complementa com um conjunto de orientações e alinhamento com outros conjuntos de regras específicos.

3.4 Norma ISO/IEC 15408

Essa norma é um *Common Criteria*, que define critérios para a avaliação de segurança de produtos e sistemas de TI, permitindo a comparação de avaliações independentes de diferentes produtos ou sistemas de acordo com os critérios *Evaluation Assurance Level* (EAL1-EAL7).

Tem como escopos análise e preservação de confidencialidade, integridade e disponibilidade da informação; foco de ameaças originadas por seres humanos, maliciosas ou não; e análise de design e processo de desenvolvimento, além de informações coletadas no processo de avaliação. Em resumo, é um guia para o desenvolvimento de produtos e sistemas seguros.

3.5 Control Objectives for Information and related Technology (CobiT)

O CobiT é um modelo e ferramenta de suporte que permite aos gestores suprirem deficiências relativas aos requisitos de controle, questões técnicas e riscos de negócios, comunicando esse nível de controle às partes interessadas. O CobiT possibilita o desenvolvimento de políticas claras e boas práticas para controles de TI em toda a organização.

Na versão 4, o CobiT estava estruturado em 4 domínios com 34 processos de controles de alto nível, e para esses processos foram criados 318 objetivos de controles necessários para analisar e atender aos requisitos de TI e, conseqüentemente, aos objetivos do negócio.

Como resultado de avaliação desses objetivos, criam-se as estratégias para mitigação de riscos existentes, baseados nos resultados obtidos.

3.6 Instrução Normativa IN-04/2008

A IN-04 é o documento oficial do governo brasileiro que provê regulação para a contratação de terceiros para a área de TI na Administração Pública Federal e que provavelmente terá adesão das demais esferas administrativas.

Publicada no mês de maio de 2008, ela agrega diversas contribuições para o processo de contratação em TI. Mas como toda lei, a IN-04 não contemplou todos os requisitos necessários, principalmente no que tange aos aspectos da SI. Em julho de 2010, após revisão, a IN-04 entra em consulta pública, onde se pode destacar a determinação de que a gestão de processos na área e as atividades de coordenação em segurança de sistemas não podem ser terceirizadas.

A IN-04 se divide em três fases, a seguir: Planejamento da Contratação, Seleção do Fornecedor, e Gerenciamento do Contrato. Para melhor compreensão, a Figura 3 traz um esboço dessas fases e suas divisões.

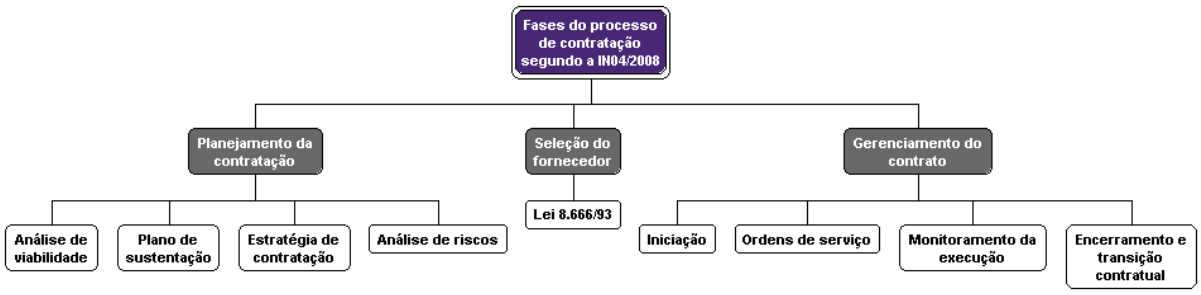

Figura 3: Esboço das fases e etapas da IN-04 [LOPES, 2004]

3.7 Outras referências

Nos tópicos anteriores foram apresentadas as principais normas e legislação que trazem contribuições para os gestores no que diz respeito a SI, podendo ser aproveitadas para balizar processos de contratação de terceiros.

Além dos documentos apresentados, este trabalho de pesquisa usou diversas outras referências no que se referem a normas, legislação, trabalhos científicos e publicações afins, as quais são apresentadas ao longo do trabalho e relacionadas nas referências bibliográficas.

Em especial, foram balizadoras do trabalho as séries de recomendações de controle de segurança (SP800-53, SP800-92 etc.) publicadas pelo NIST (National Institute of Standards and Technology), que podem ser acessadas por meio da URL http://csrc.nist.gov/publications/PubsSPs.html; e os artigos que relacionam terceirização e SI, do Sans Technology Institute (http://www.sans.edu/resources).

4. Mitigando os Riscos Envolvidos nos Processos de Terceirização da TI

4.1 Aspectos Gerais

Terceirização de serviços de TI é um dos segmentos de negócio que mais tem crescido, como também, discutido mundo afora, principalmente na Administração Pública. Essa discussão decorre de diversos motivos, sendo que alguns são mais enfatizados e outros nem tanto. Um dos motivos que não tem recebido grande ênfase por parte de gestores, mas de suma importância no contexto da terceirização e que nos leva a escrever este trabalho, é a gestão de riscos no que tange à alocação de pessoas para a prestação de serviços de TI em áreas onde a informação manipulada é sensível e estratégica para o negócio da organização.

Como a terceirização da TI, pessoas que não são diretamente responsáveis pelo negócio passam a ter acesso aos dados sensíveis da organização e, portanto, os desafios frente à Segurança da Informação (SI) são inevitáveis, visto que os processos de negócio já não se encontram somente nas mãos da organização, mas também da empresa contratada, demandando assim um maior controle sobre a mesma.

O processo de terceirização da TI requer uma nova visão da segurança dos dados e de uma gestão de riscos de sucesso. Qualquer negócio possui uma parcela de risco, mas quando se trata de terceirizar a manipulação da informação, essa parcela toma proporções que demandam o uso de regras (definição de políticas de segurança), normas e boas práticas legais (cláusulas contratuais, transferência de riscos etc.), controle e monitoração (uso de metodologias) de forma mais efetiva.

É fato que, em sua maioria, as ameaças frente às vulnerabilidades encontradas nos ativos da organização (pessoas, processos, tecnologia e ambiente físico) encontram-se internamente à mesma, ou seja, normalmente os ataques são protagonizados pelos próprios funcionários.

As ameaças podem ser intencionais ou não (caso da falta de conhecimento). Como exemplo, pode-se citar a situação em que a empresa contratada envia mão-de-obra não qualificada aos objetivos da organização.

Com o processo de terceirização da TI, as fragilidades aumentam em muito e podem ser um problema difícil de resolver, podendo haver impactos não mensuráveis, e muitas vezes são avisadas por meio de um simples incidente que, se não tratado, transforma-se em desastres e até mesmo em uma catástrofe.

Ainda, como mitigar/reduzir os riscos quando detectadas atividades maliciosas partindo de empregados confiáveis e que estão autorizados a utilizar os dados e necessitam ter acesso aos mesmos, a fim de fazerem seus trabalhos diários?

Quando se trata de terceirização, esse problema é ampliado pelo fato de que os usuários que acessam os dados não têm o mesmo compromisso com a organização.

A penalização legal e jurídica da pessoa física (funcionário terceirizado) que violou os dados ou agiu maliciosamente nem sempre é possível, seja por falta de provas ou porque a empresa que é contratada apenas o demite.

4.2 Tabulando as Melhores Práticas

O que se segue é um conjunto de tabulações que agregam fragilidades não somente aos processos de terceirização da TI, mas da SI como um todo e tem como foco dar visibilidade ao gestor público, dos riscos envolvidos para o negócio.

Associado a cada tabulação são apresentadas as contramedidas ou boas práticas, focando em normas, padrões e controle, de modo que os riscos envolvidos possam ser mitigados.

Está fora do escopo deste trabalho, apresentar como boas práticas, questões operacionais ou de procedimentos, mas apenas a indicação de qual norma, metodologia ou lei/regulamentação melhor aborda a resolução do problema e, ou apresenta melhores práticas.

4.2.1 O que terceirizar na TI

Contextualização:

O ponto inicial para se mitigarem os riscos relativos à Segurança da Informação é fazer uma análise de risco visando identificar quais áreas são mais vulneráveis e relevantes, portanto, que se encontram sujeitas a ameaças por parte de terceiros quando da manipulação de informações ou da ação sobre processos de TI que possuem alto grau de sensibilidade quanto à apropriação indébita do dado, da perda do sigilo e da integridade, que, se ocorrendo, poderá gerar impactos para o negócio da organização.

Na maioria dos casos, o negócio gerido pela organização é suportado pelos processos de TI, o que demonstra, portanto, que a TI é um elemento estratégico para a organização, sendo, assim, desejável que a SI tenha certa relevância e esteja em uma das perspectivas do mapa estratégico de TI e da Organização.

Em geral, as áreas da TI que merecem maiores atenções são as de administração de banco de dados (base de dados bancários, de tributos, benefícios, sistemas de votação, sistemas militares e de inteligência, entre diversos outros sistemas de missão crítica), administração de sistemas de controle de acesso e autorização (criação de *logins* de rede, permissões a sistemas que usam base de dados sensíveis, acesso a sistemas de arquivos, entre outros), administração de software de segurança (*firewall*, sistema de prevenção de intrusão, sistema de prevenção de vírus e códigos maliciosos, entre outros).

Boas Práticas:

A avaliação de riscos para o negócio em relação a falhas de segurança em TI deve ser uma prática a ser adotada de forma periódica. O nível dessa avaliação normalmente está associado à criticidade do dado, do ativo, ou do processo que se deseja proteger e de que fonte de ameaça. Porém, para

qualquer contexto que inclua processos de terceirização, o uso da metodologia OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) como um todo, trará bons resultados.

A OCTAVE compreende uma abordagem de Gestão dos Riscos de Segurança da Informação desenvolvido pelo *Software Engineering Institute (SEI)*, da Universidade de Carnigie Mellon. Em essência, é feita uma avaliação quanto ao Risco Operacional, às Práticas de Segurança, e a Tecnológica. Complementa-se com a aplicação de três fases, que compreende a criação de um perfil de ameaça do ativo, a identificação da vulnerabilidade da infra-estrutura, e conclui-se com o desenvolvimento da estratégia de segurança e dos planos de segurança da informação.

A OCTAVE já contribui muito no processo de gestão de riscos, porém os estudos das normas ISO 27005/30001 e AS/NZ4360 serão essenciais na complementação do trabalho de análise de riscos e dos pontos de decisão.

O CobiT em seus objetivos de controle, por meio do processo PO9 (Avaliar e Gerenciar Risco, também é uma boa referência de boas práticas e não deve ser deixado de lado.

4.2.2 Contratação de Terceiros

Contextualização:

Um segundo critério, ao qual em principio não é dada muita atenção, é o processo de contratação do terceiro ou da empresa que prestará os serviços de TI e mais especificamente da pessoa física que prestará o serviço, seja internamente ou externamente à organização. Fazer uma boa contratação já é um grande passo na mitigação dos riscos de SI.

As organizações terceirizam os seus serviços normalmente, mediante a contratação de uma empresa, e os serviços são operacionalizados por pessoas. Na Administração Pública, para que empresas sejam contratadas, devem-se seguir as leis que regem os processos licitatórios.

Boas Práticas:

Para contratar bem, é necessário cumprir, no mínimo, o que determina a Lei 8.666/93, que institui normas para licitações e contratos da Administração Pública, a Lei 10.520/02 (pregão presencial), o Decreto 5.450/05 (pregão eletrônico) e a Instrução Normativa Nº 4/08, que dispõe sobre o processo de contratação de serviços de TI pela Administração Pública Federal.

Adicionalmente, o edital para a contratação de terceiros deve prever que a contratada e os recursos por ela alocados para a prestação de serviços deverão estar alinhados com as políticas de SI vigentes, além de ser pactuado um termo de sigilo entre a organização que contrata os serviços e o contratado (empresa e o recurso humano diretamente alocado para o serviço).

A norma ISO 27001, em seu Anexo A (seção A8), tabula algumas boas práticas para o processo de contratação. O CobiT, em seus objetivos de controle, mediante o processo P07 (Gerenciar Recursos Humanos de TI) e DS7 (Gerenciar Serviços Terceirizados), baliza algumas regras de controle e gerenciamento passíveis de estarem como obrigações da contratada.

4.2.3 Rastros de Auditoria

Contextualização:

Avaliados os riscos de negócio para definir o que terceirizar dentro da TI e posteriormente contratar com base nessa avaliação, o próximo passo que deverá estar pronto são os mecanismos para monitorar ações frente às atividades sobre os recursos computacionais, principalmente os não autorizados. Gerar rastros com base nas ações, onde se pode identificar o que foi feito, por quem foi feito, como foi feito**,** associados aos dados cronológicos**,** é de suma importância para que se possa responsabilizar ações maliciosas ou não condizentes com as regras e objetivos de negócio da organização.

Boas Práticas:

Mecanismos baseados em biometria associados ao identificador do sujeito (usuário ou sistema) são os mais indicados para garantir a verdadeira autenticidade do sujeito que efetuou a ação ou transação junto ao sistema computacional. Em caso de uso malicioso, a utilização de rastros de auditoria claros e bem definidos pode ser um elemento legal de prova em processos administrativos ou judiciais.

Pode não ser tão simples de identificar ou provar o ato malicioso, portanto, para mitigar ainda mais os riscos, além do emprego de biometria, o uso de certificados digitais na aferição da autenticidade é uma boa prática, visto que um dos objetivos dos certificados digitais é garantir a propriedade do não-repúdio ou irretratabilidade da ação.

Qualquer informação de auditoria terá maior aceitabilidade jurídica se o processo encontra-se definido nas políticas da organização e as informações de cronologia estão sincronizadas e auditadas através da Hora Legal Brasileira [DIAS *et al*., 2003; MELO, 2008] do Observatório Nacional, principalmente quando a origem da operação computacional encontra-se externa à organização e o recurso que sofre a ação, interno à organização.

A norma ISO 27001 em seu item 10 do Anexo nº 10 tabula alguns itens para a monitoração e detecção de atividades não autorizadas de processamento das informações, tais como: registros de auditoria, monitoramento do uso de sistemas, proteção das informações de registro, registros de administrador e de operador, registros de falhas e sincronismo de relógio.

Um monitoramento de conformidade das atividades de TI é provido pelo *framework* CobiT através do domínio ME (Monitoração e Avaliação), e tê-lo como aliado no processo é uma boa prática. Em verdade, o CobiT trata a auditoria em praticamente todos os seus objetivos de controle.

4.2.4 Controle de acesso, Autorização e Classificação da Informação

Contextualização:

É fato que em organizações, sejam elas privadas ou públicas e até mesmo em informática residencial, o acesso a sistemas computacionais como um todo é restrito a pessoas e objetos devidamente autorizados. Esse controle de acesso, seja físico ou lógico, tem como objetivo primordial a proteção do ativo e da informação.

Mas como mitigar os riscos de SI e detectar atividades maliciosas quando os funcionários da organização estão devidamente autorizados ao uso dos recursos computacionais e têm acesso aos dados?

Quando se trata de terceirização, esse problema é ampliado pelo fato de que os usuários que acessam os dados podem não estar dentro da organização, podendo estar em qualquer parte do mundo e não têm o mesmo nível de comprometimento e responsabilidade de um funcionário efetivo.

Outro fato que deve ser levado em consideração pela organização é a classificação da informação. Deve-se determinar o grau de acesso e sigilo da mesma, ou seja, quem pode ou não ter acesso à mesma e ao conhecimento de seu conteúdo.

Boas práticas:

Garantir a segurança dos ativos e dos dados não é uma tarefa fácil e tampouco se pode determinar que os controles aplicados são 100% seguros. O básico é gerar controles para que o acesso seja feito somente pelas pessoas ou objetos computacionais que realmente foram autorizados. A autenticidade desse acesso também deve ser garantida.

Para se mitigar o que foi posicionado anteriormente, o mínimo que se deve dispor é o controle usuário/senha (conhecida como autenticação fraca), mas o desejável é que, além desse mecanismo, processos de autenticação e autorização por meio de dispositivos biométricos e certificados digitais estejam disponíveis, tanto para o acesso físico, como lógico. Para o acesso lógico, o uso de certificados digitais também é desejável.

Um dos grandes pontos de falha em processos de terceirização é o livre poder discricionário atribuído ao executor dos serviços de TI, que inclui a administração do controle de acesso, banco de dados e da própria segurança. Conforme Lampson [1971], nesse modelo (*Discricionary Access Control - DAC*), o controle de acesso ou permissões de um objeto pode ser repassado de um usuário para outro, bastando que o mesmo seja o dono do objeto, gerando, assim, sérias falhas de segurança, uma vez que pode ocorrer de ser atribuído a um usuário o direito de acessar informações cuja classificação não é condizente com o seu perfil.

Para minimizar os riscos e limitações do poder discricionário, associado às características que permitam uma maior escalabilidade e uma administração mais

otimizada do controle de acesso, o uso do mecanismo de acesso/direitos baseado em papéis – o RBAC (*Role Based Access Control*) [FERRAIOLO *et al.*, 1995], é uma opção no fortalecimento da Segurança da Informação, principalmente em situações em que os serviços terceirizados são executados distribuidamente entre as diversas áreas da organização. Os modelos DAC e RBAC podem coexistir, robustecendo o controle.

Implementar processos para Gestão de Identidades permite definir uma identidade digital a uma entidade (pessoas e processos). A essa identidade, associa atributos, permitindo a sua verificação globalmente dentro da instituição. Isso se mostra importante, porque um fornecedor ou terceirizado poderá assumir diferentes papéis na organização; portanto, seus atributos de direitos de acessos aos recursos devem acontecer conforme sua identidade e mobilidade dentro da organização.

A norma ISO 27001, em seu Anexo nº 7, Item 2, trata da classificação da informação e traz diretrizes de boas práticas para assegurar que a informação receba um nível adequado de proteção. No Anexo nº 11 são esboçadas diretrizes para o controle de acesso e autorização, contemplando os mais diversos objetos que demandam tais requisitos.

O CobiT, embora não trate diretamente com controle de acesso, no objetivo de controle PO2.3 estabelece um esquema de classificação de dados aplicável a toda organização com base na importância e na confidencialidade dos dados corporativos.

4.2.5 Integridade, Confidencialidade e Disponibilidade

Contextualização:

A integridade, a confidencialidade e a disponibilidade são os três pilares (ou propriedades) estruturais da SI. A autenticidade e o não-repúdio complementam essa estrutura, e todos já foram sucintamente explanados no item 2.1 do referencial teórico deste trabalho.

Na atual conjuntura, a TI é parte estratégica de qualquer negócio. Portanto, a SI passa a ser também um elemento estratégico para a TI. Desse modo, a garantia dessas propriedades – ou seja, a integridade, confidencialidade e disponibilidade junto aos sistemas de informação – é fundamental para a organização.

Nas médias e grandes organizações, a terceirização dos serviços é uma realidade e a operacionalização dos serviços pode ser local ou mediante o uso dos meios de comunicação (Internet, ambiente de rede local etc.). Nesse contexto, onde o acesso parte da rede de comunicação, seja local ou remota a organização, a segurança física é irrelevante e os aspectos de proteção lógica, tendo como objetivo garantir os pilares da SI, torna-se fundamental.

As boas práticas a seguir são referências mitigadoras para o problema.

Boas práticas:

As boas práticas que visam resguardar os ativos quanto à integridade, confidencialidade e sua disponibilidade devem se lançar de um conjunto de ações que compreende a implementação de controle e monitoração já tratados anteriormente nos itens 4.2.3 (auditoria) e 4.2.4 (autorização, controle de acesso e classificação dos dados).

É de suma importância informar aos fornecedores as suas obrigações para a proteção e acesso à informação, além de estabelecer os controles de acesso adequados, de modo que o usuário tenha apenas os direitos mínimos para a execução da tarefa.

4.2.6 Políticas de Segurança e Procedimentos

Contextualização:

Vivemos em um mundo de regras e procedimentos. Proceder conforme a lei é seguir uma regra, ou seja, a lei. Assim, as regras visam garantir o controle legal e a ordem das coisas.

Pode-se definir que políticas de segurança são regras que devem ser criadas para garantir e deixar claro o que é permitido, ou o que é proibido, visando garantir o uso adequado e seguro dos ativos da organização ora providos pela TI.

A política é criada, homologada e divulgada conforme os interesses da organização. A partir do momento em que essas três etapas são concretizadas e as pessoas tomam ciência dos seus direitos e deveres com base nas regras, a infração a qualquer uma delas deve cominar em penalidades, podendo ser administrativas ou judiciais, conforme a gravidade.

Os procedimentos são códigos de práticas para garantirem a execução da política ou das regras estabelecidas.

Boas Práticas:

Em ambientes de TI onde há terceirização, definir políticas de segurança é essencial. A política é um documento que deve ser oficializado e dado conhecimento no contrato com o fornecedor de serviço, devendo, obrigatoriamente, todas as pessoas que manipulam ativos da organização ter ciência das regras e assinar um termo.

A assinatura do termo, combinada com outras evidências (informações de auditoria, por exemplo), é a garantia que a organização terá, caso seja necessário recorrer administrativamente junto ao fornecedor de serviços ou até mesmo junto à justiça em caso de ações maliciosas, inadequadas ou que estejam em desacordo com as regras.

Porém, nada adianta a existência de regras, se não forem disponibilizados os recursos necessários para o cumprimento das mesmas, seja mediante procedimentos ou controles.

Também não se pode penalizar quando não se consegue provar a infração. Assim, quando cabível, para cada regra imposta, devem-se prover dispositivos que gerem legalmente rastros de auditoria – em outras palavras, provas legais e não contestáveis.

Para que uma política de segurança seja efetiva, as boas práticas referentes a rastros de auditoria e para o controle de acesso expostos respectivamente nos itens 4.2.3 e 4.2.4 são extremamente importantes.

E muito comum a situação onde o fornecedor passa a ter acesso aos sistemas computacionais da organização contratante e quando do desligamento ou encerramento do contrato, as pessoas que lá prestavam serviço ainda continuam com acesso irrestrito por grande período (inclusive correio eletrônico). A causa decorre da ausência de políticas combinadas com procedimentos.

4.2.7 Sistema de Gestão da Segurança da Informação

Contextualização:

A norma ABNT NBR ISO/IEC 27001:2006 compreende um conjunto de requisitos para o desenvolvimento de um Sistema de Gestão da Segurança da Informação (SGSI), que consiste num *framework* de gestão baseada no gerenciamento de risco para estabelecer, implementar, operar, monitorar de forma proativa, revisar, manter e otimizar a segurança da informação de uma organização.

O SGSI é uma ferramenta ampla de gestão, que inclui, por exemplo, definição da estrutura organizacional, definição de papéis e políticas de segurança. Possibilita sistematizar a gestão de riscos e descrever as melhores práticas para tratá-los.

Boas Práticas:

Desenvolver, implementar e colocar em prática os diversos componentes de um SGSI já se trata de uma boa prática para garantir a segurança dos ativos das organizações frente às possíveis ameaças.

O que se deve fazer é garantir que todas as áreas tratadas no SGSI sejam efetivamente implementadas, operacionalizadas e monitoradas conforme o ciclo PDCA.

Um processo de monitoração e manutenção contínua do SGSI se faz necessário para garantir a execução do que foi estabelecido; e é muito importante que toda a equipe esteja integrada ao processo e que a importância do mesmo esteja clara para todos.

O uso obrigatório de *checklists* é um dos diversos itens que podem garantir a execução das premissas de um SGSI. Sempre que possível, sua execução deve envolver alternância entre executores visando eliminar erros e vícios desenvolvidos. Periodicamente, um gerente da área deve fazer a mesma verificação de modo a garantir ainda mais que o que está sendo colocando em

prática seja feito de forma correta. O *backup* dos dados e a administração de direitos (controle de acesso, regras de *firewall*, etc.) são itens de suma importância que podemos destacar.

4.2.8 Recomendações Gerais

Até o momento, foram apresentadas as melhores práticas conforme cada segmento da SI. O que se segue são uma tabulação e um conjunto disperso de melhores práticas que agregam contribuições balizadoras para o processo de contratação de terceiros associados a SI:

- Como primeiro ponto, é muito importante que, num processo de contratação de fornecedores de serviços, o mesmo tenha conhecimento detalhado, e de forma oficial, de suas obrigações para a proteção e confidencialidade dos dados da organização;

- A organização contratante de fornecedores de serviços deve avaliar e decidir que tipos de informações serão compartilhadas e fazê-lo apenas na medida necessária para a execução dos serviços atribuídos, além de impor medidas adequadas para assegurar a confidencialidade e integridade dos dados;

- Deve ser compactuado entre a organização e o fornecedor que quaisquer dados ou informações da organização e que estejam em poder do fornecedor devam ser destruídos após término do contrato;

- É importante que, em um processo de terceirização, a organização contratante estabeleça contratualmente penalidades e até mesmo cláusulas indenizatórias para casos de omissão e violação de políticas de segurança, durante e após o término do contrato. No entanto, é de suma importância que as responsabilidades e penalidades atribuídas sejam exeqüíveis e que estejam em sintonia com a lei;

- Sempre que possível, a organização deve identificar e classificar as informações e os tipos de mecanismos de segurança a serem obrigatoriamente utilizados pelo fornecedor de serviços de exercício do contrato;

- Dar conhecimento ao fornecedor de serviços, das leis e regulamentos relativos a SI;

- Estabelecer controle de acesso do fornecedor sobre as informações e impor restrições à forma de como a informação pode ser utilizada, transferida ou compartilhada e, essencialmente, implementar mecanismos que gerem rastros de auditoria sobre os procedimentos executados pelo fornecedor sobre os dados e recursos computacionais.

5. Conclusão

Este trabalho apresentou algumas diretrizes e referências de SI que devem ser consideradas em processos de terceirização, visando à proteção dos ativos da organização, no que tange a garantir a integridade, confidencialidade e disponibilidade da informação.

Teve como base o uso da legislação, normas e padrões internacionais, além de trabalhos relacionados à segurança e terceirização em TI.

Espera-se que, com o exposto, os gestores tenham o mínimo de subsidio para balizarem suas ações e contramedidas de segurança e análise de riscos frente à contratação de terceiros que interagirão diretamente com os ativos da organização.

As ações acima listadas devem ter suas ações determinadas por meio de um fluxo estruturado, bem como por sua análise crítica e monitoramento continuo, ou seja, da contratação, durante o seu exercício, e procedimentos proativos no desligamento dos terceirizados, mirando sempre do grau de importância de cada “caixa” estratégica suportado por esses ativos.

Conforme histórico levantando em Leite [1994], processos de terceirização já ocorrem há décadas, mas somente nestes últimos anos o assunto tem ganhado foco, principalmente no que diz respeito à área de TI; portanto, o assunto é longo é não se esgota aqui.

Espera-se que outros trabalhos afins sejam desenvolvidos visando um maior debate e que os processos de terceirização sejam equacionados, ofertando menor custo, que sejam eficientes e eficazes e que propiciem proteção aos ativos da organização.

6. Referências

ABREU, M. F. "**Os riscos da terceirização e da adoção de novas TIs e suas relações com os riscos para as estratégias competitivas das organizações**". Tese de Doutorado, Universidade Federal do Rio Grande do Sul, 2009.

ALBERTS, C.; DOROFEE, A. "**An Introduction to the OCTAVE Method**". Carnegie Mellon University, Software Engineering Institute, CERT Coordination Center, 2001.

AS/NZS 4360; AS/NZS 4360:2004. **"Risk Management"**. Australian/New Zealand Standard, 2004.

AUBERT, B. A.; RIVARD, S.; PATRY, M. "**Assessing the Risk of IT Outsourcing**", maio-1998. Disponível em URL: <http://www.cirano.qc.ca/pdf/publication/98s-16.pdf>. Acesso em: ago. 2010.

CORDON, R. "**How to mitigate the security risks of outsourcing**". Computer Weekly Magazine, Dec. 2007.

DIAS, J. S.; CUSTÓDIO, R. F.; DEMÉTRIO, D. B. "**Sincronização Segura de Relógio para Documentos Eletrônicos**". Anais do XXI Simpósio Brasileiro de Redes de Computadores, p. 586-587, 2003.

FERRAIOLO D.; CUGINI, J.; KUHN, D. R. "**Role Based Access Control: Features and Motivations**". Computer Security Applications Conference, 1995.

FINK, D. "**A Security Framework for Information Systems Outsourcing**". Information Management & Computer Security, v. 2, nº 4, p. 3-8, 1994.

IAM. "**Information Security Assessment Methodology**". National Security Agency. Information Assurance Directorate, 2001.

ISO 27001. ABNT NBR ISO/IEC 27001:2006. "**Sistemas de gestão de segurança da informação – Requisitos**". Associação Brasileira de Normas Técnicas, 2006.

ISO 27002. ABNT NBR ISO/IEC 27002:2005. "**Código de prática para a gestão da segurança da informação**". Associação Brasileira de Normas Técnicas, 2005.

ISO 27005. ABNT NBR ISO/IEC 27005:2008. "**Gestão de Riscos de Segurança da Informação**". Associação Brasileira de Normas Técnicas, 2008.

ISO 31000. ABNT NBR ISO/IEC 31000:2009. "**Gestão de Riscos Princípios e Diretrizes**". Associação Brasileira de Normas Técnicas, 2009.

íTALO, L. **"Instrução Normativa 4"**, agosto de 2009. Disponível em URL: <://italolopes.wordpress.com/2009/08/09/instrucao-normativa-4-parte-1>. Acesso em: set. 2010.

KADAKIA R. "**Collaborative Security Strategies in an Outsourced, Cross-Agency Web System**". SANS Institute, As part of the Information Security Reading Room, 2001.

KHALFAN, A. M. Khalfan. "**Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors**". International Journal of Information Management 24, p. 29-42, 2004.

LAMPSON, B. W. "**Protection**". 5th Princeton Conference on Information Sciences and Systems, p. 437, 1971.

LANDWEHR, C. E. "**Computer Security**". Publicação Online, Springer-Verlag, 2001.

LEITE, J. C. **"Terceirização em Informática".** São Paulo: Makron Books, 1994.

PRADO, E. P. V. "**Terceirização da Tecnologia da Informação: uma avaliação dos fatores que motivam sua adoção em empresas do Setor Industrial de São Paulo**". Dissertação de Mestrado, Universidade de São Paulo, 2000.

MELO, R. C. L. "**Eficácia probatória dos documentos digitais no âmbito da auditoria tributária**". Revista Brasileira de Contabilidade, nº 164, p. 77, 2008.

NIACAP. "**National Information Assurance Certification and Accreditation Process**". National Security Telecommunication and Information Systems Security Committee, 2000.

NIST. "**Federal Information Processing Standards 102**". Guidelines for Computer Security Certification and Accreditation. National Institute of Standards and Technology, 1983.

OLIVEIRA, F. C.; FILHO, J. L. S. "**Fatores de Riscos Associados à Terceirização de TI no Setor Público**". III SEGeT – Simpósio de Excelência em Gestão e Tecnologia, 2006.

PRADO, E. P. V. "**Terceirização da Tecnologia da Informação: uma avaliação dos fatores que motivam sua adoção em empresas do setor industrial de São Paulo**". Dissertação de Mestrado, Universidade de São Paulo, 2000.

SANTIN, A. "**Teias de Federações: uma abordagem baseada em cadeias de confiança para autenticação, autorização e navegação em sistemas de larga escala**". Tese de Doutorado, Universidade Federal Santa Catarina, 2004.

SCHNEIER, B. "**The Case for Outsourcing Security**". Supplement to IEEE Computer Magazine, 2002.

SWANSON, M. "**Self-assessment Guide for Information Technology Systems**". National Institute of Standards and Technology, 2000.