Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Especialização em Gestão da Segurança da Informação e Comunicações

LEOCLIDES MILTON ARRUDA

A TERCEIRIZAÇÃO E A SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NO SERVIÇO PÚBLICO

Brasília

2010

LEOCLIDES MILTON ARRUDA

A TERCEIRIZAÇÃO E A SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NO SERVIÇO PÚBLICO

Brasília

2010

LEOCLIDES MILTON ARRUDA

A TERCEIRIZAÇÃO E A SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NO SERVIÇO PÚBLICO

Monografia apresentada ao Departamento de Ciência da Computação da Universidade de Brasília como requisito parcial para a obtenção do título de Especialista em Ciência da Computação: Gestão da Segurança da Informação e Comunicações

Orientador
Professor Dr. Jorge Henrique Cabral Fernandes
Departamento de Ciência da Computação
Universidade de Brasília – UnB

Brasília
2010

Monografia de Especialização defendida sob o título *"A terceirização e a segurança da informação e comunicações no serviço público"*, defendida por Leoclides Milton Arruda e aprovada em 26 de julho de 2010 em Brasília-DF, pela banca examinadora constituída pelo(a)s professore(a)s e pesquisadore(a)s:

Orientador
Professor Dr. Jorge Henrique Cabral Fernandes
Departamento de Ciência da Computação
Universidade de Brasília

Professora Dra.Claudia Lyrio Canongia
Pesquisadora do INMETRO,
Cedida ao DSIC/GSIPR

Professor Dr. Marcelo Felipe Moreira Persegona
Faculdade SENAC-DF

Dedicatória

Aos meus pais Maria Eduarda e João Arruda; a minha querida esposa Alice, por sua compreensão; as minhas filhas Giany e Priscila e aos meus genros Bruno e Diego, pelo apoio em todos os momentos desta importante etapa em minha vida.

Agradecimentos

- Gostaria de externar meus agradecimentos primeiro a Deus;
- Aos meus amigos de sala de aula e professores que transmitiram seus conhecimentos valiosos e fizeram valer o nome que lhes é dado: "Educadores";
- Ao meu Orientador, professor Jorge Henrique Cabral Fernandes, pela atenção, paciência e dedicação prestada nas diversas fases do trabalho.
- Aos colegas de trabalho; meus amigos Samuel da Mata e Aparecida Santana; Reinaldo Silva Simião e Gilmar Santos; a todos que direta ou indiretamente ajudaram na realização e conclusão deste trabalho.

Glossário

A

APF - Administração Pública Federal

C

CUT - Central Única dos Trabalhadores

D

DAC - Discretionary Access Control

DOU - Diário Oficial da União

G

GSI -Gestão de Segurança da Informação

I

ISO - International Organization for Standardization

M

MSS - Managed Security Services

MAC - Mandatory Access Control

MoREQ - Model Requirements for the Management of Electronic Records - MoReq

e-ARQ - Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos

P

PPT - Pessoas, Processos e Tecnologias

RBAC - Role-Based Access Control

S

SGAE - Sistema de Gestão de Arquivos Eletrônicos

SIC - Segurança da Informação e Comunicações

SIGAD3 - Sistema Informatizado de Gestão Arquivística de Documentos Digitais

SLAs - Service Level Agreement

T

TI - Tecnologia da Informação

Sumário

Lista de Figuras

RESUMO

Em nome da leveza na estrutura, da agilidade e da flexibilidade, o serviço público, de modo geral, tem se caracterizado nas últimas décadas pelo aumento contínuo das taxas de terceirização de serviços em áreas não só operacionais, mas também estratégicas. A maioria das organizações públicas tem hoje sua área de processamento de dados e de gestão da informação entregue a grandes empresas, que prestam serviços aos mais diferentes setores públicos e privados do País. Com o advento da internet e, principalmente a partir do "*bug* do milênio", novos parâmetros de segurança de dados e da informação foram adicionados às preocupações da gestão da empresa moderna. No serviço público, em particular, estudos recentes mostram a grande vulnerabilidade da maioria das organizações públicas quanto à gestão e segurança da informação e comunicações. Este trabalho analisa, à luz da literatura, a vulnerabilidade da segurança da informação e comunicações no serviço público, correlacionado-a com a expansão da terceirização de áreas estratégicas nas organizações públicas.

Palavras chave: Segurança da informação; Terceirização; Serviço público.

ABSTRACT

On behalf of lightness in structure, agility and flexibility, public service, in general, has been characterized, in recent decades, by the steady increase in the rate of outsourcing services in areas not only operational but also strategic. Most public organizations today have their area of data processing and information management delivered to large enterprises, providing services to many different public and private sectors in the country. With the advent of the Internet, and principally from the "millennium bug", new parameters for data security and information were added to the concerns of modern business management. In the public service, in particular, recent studies show the great vulnerability of most public organizations in management and information security and communications. This study examines, in light of the literature, the vulnerability of information security and communications in public service, it correlated with the expansion of outsourcing of strategic areas in public organizations.

Keywords: Information Security, Outsourcing, Public service.

Introdução

Em um mundo cada vez mais globalizado e competitivo, a Segurança da Informação e Comunicações tem sido um tema da maior preocupação, em especial pelos órgãos de controle como na administração publica federal[1]. É inegável que as empresas têm despendido enormes recursos para precaver-se contra as vulnerabilidades dos seus negócios. Os aspectos que mais as preocupam são: a velocidade da informação, que em alguns casos dificulta a tomada de decisão, a exposição a riscos de vazamento de informações, além da perda ou adulteração de dados.

Nenhuma organização consegue livrar-se de grandes investimentos na área de segurança da informação e comunicações, sob pena de perder o seu papel social ou importância econômica. No setor público, onde a principal missão é garantir a soberania e desenvolvimento, social, econômico e financeiro da nação, essa necessidade se torna muito mais evidente.

Grande parte dos investimentos dos investimentos que as Organizações no Brasil tem feito nos últimos anos está voltada para a área de tecnologia[2]. A construção de redes e sistemas de acessos mais seguros tem sido uma preocupação constante. Todavia, novos estudos têm demonstrado que a falta de conscientização, capacitação, treinamentos e, principalmente, de comprometimento da alta administração, têm tornado vulneráveis e deficientes a grande maioria dos programas do governo por falta de uma política de Segurança da Informação e Comunicações na APF é o que aponta o TCU em 65% dos Órgãos Públicos[3].

Não se pode pensar em segurança como um programa de construção e aplicação estanque. Garantia de segurança exige constantes ajustes e testes que só pessoas bem treinadas, capacitadas e conscientes são capazes de desenvolver. Para garantir a disponibilidade, integridade, confidencialidade e autenticidade, se faz necessário um conjunto de ações por parte de todos os entes públicos. Programas e equipamentos modernos por si só não garantem a segurança da informação e

[1] Ver Folha de SP de 08.09.2010.
[2] Ver Revista CIO Brasil, de 28/12/09.
[3] Ver R7 publicado em 08/09/2010.

comunicações se não estiverem acompanhados de minuciosa investigação e identificação de suas vulnerabilidades. (Ministério do Planejamento e Gestão – Agosto/2000).

Segundo o ministro do Planejamento, Guido Mantega, em entrevista publicada por O Trabuco (2004), a decisão de contratar 41 mil servidores públicos federais "*é um movimento de desterceirização do setor público*". Segundo ele, havia uma "*ilusão*" de que o número de funcionários públicos vinha sendo reduzido nos últimos anos, mas na verdade eles vinham sendo substituídos por terceirizados. "*Concluímos que isso diminuía a performance do Estado*", disse. "*Por isso, optamos por contratar servidores habilitados para a função, profissionalizar o serviço público*." Na verdade o próprio Governo Federal, por conta do Termo de Conciliação Judicial – Processo nº 00810-2006-017-10-00-7, se vê obrigado a desterceirizar o serviço publico.

Napoleão Hill escreveu em um de seus livros (A Lei do Triunfo, p.114) que "a melhor compensação por uma coisa que realizamos é capacidade que adquirimos para fazê-la ainda mais e melhor."

Diante da constatação desta situação, vivenciada inclusive pelo Autor, na sua atividade em órgão da Administração Direta da União mostra-se a necessidade de compreender melhor os processos e consequências da terceirização, sob o ponto de vista da segurança da informação e comunicações.

2. Requisitos Pré-pesquisa

2.1. Objetivos

2.1.1. Objetivo Geral

Analisar a expansão do processo de terceirização como fatores de risco à segurança da informação e comunicações no serviço público no Brasil.

2.1.2. Objetivos Específicos

São objetivos específicos da pesquisa

1. Analisar o atual cenário da política de Segurança da Informação e Comunicações nas instituições públicas;
2. Buscar e analisar as relações da terceirização de serviços, com a política de segurança da informação e comunicações na APF.

2.2. Justificativa

O ultimo século foi marcado com o avenço tecnológico com profunda repercussão na vida das pessoas e das empresas. Viver sem as vantagens advindas desses avanços é no mínimo impensável. *Sites*, *e-mails*, *downloads* de arquivos etc, fazem parte do dia-a-dia das empresas e das pessoas.

Contudo o tráfego de documentos e dados necessita de estrutura adequada para que estes se mantenham seguros, íntegros e disponíveis, a fim de cumprir com a tão almejada facilidade de acesso a aquilo que se precisa para desenvolver as atividades, sejam elas econômicas ou sociais.

A necessidade da criação de ambientes seguros tem exigido das empresas privadas e públicas a adoção de medidas de proteção contra ameaças aos seus ativos.

O Decreto nº. 3.505 de 2000 instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal e a Instrução Normativa nº 1 de 2008 disciplina a Gestão da Segurança da Informação e Comunicações – (GSIC), na Administração Pública Federal direta e indireta.

A Constituição da Republica Federativa do Brasil, de 1988, bem como outras Normas Federais: Lei 9507 de 12 de novembro 1997; O Decreto 3.505, de 13 de junho de 2000; Decreto 4.553 de 27 de dezembro de 2002 e ainda a Resolução n.º 20, de 16 de julho de 2004, demonstram claramente a preocupação com a disponibilidade e a segurança da informação.

Todavia, as pessoas sempre foram uma preocupação para a segurança da informação, tanto nas empresas como na área de governo. A terceirização dos serviços públicos pode representar uma vulnerabilidade.

De acordo com a Consultoria IDC (Revista Risk Report edição de 11.08.2006, Seção: Soluções – Gestão), o segmento de MSS – *Managed Security Services* é o que mais cresce no mundo na área de segurança. Em 2006, os gastos com Segurança da Informação atingiram 38 bilhões de dólares mundialmente, sendo que 45% desse montante foram para as mãos dos provedores de serviços. Do restante, 35% ficaram com a área de hardware e 19% com a de software.

Vivemos um momento de crescimento econômico, onde o Brasil se destaca no cenário internacional e já aparece como o terceiro maior mercado de microcomputadores do mundo. A sociedade utiliza cada vez mais a rede mundial de computadores como ferramenta de trabalho, estudo e lazer, enquanto investimentos em tecnologia da informação e telecomunicações permitem ao Governo avançar na eficiência operacional e na melhoria do relacionamento e do atendimento aos cidadãos. (Programa e-Brasil – Governo Eletrônico).

Estudos da IDC (IDC Brasil Conferência 2009: TI e Telecom no Governo Brasileiro), revelam que atualmente, o governo é responsável por uma grande fatia da demanda de tecnologia da informação e telecomunicações no mercado brasileiro. Apesar disso, o Brasil vem perdendo posições no ranking mundial de governo eletrônico e, também, muito vem sendo discutido sobre o papel do governo como regulador e impulsionador do setor de Tecnologia da Informação – (TI), no país, desoneração da mão-de-obra para as empresas exportadoras de tecnologia e

aprimoramento do processo de contratação de serviços de tecnologia da informação pela administração pública direta.

Embora alguns setores da Administração Pública Federal – (APF) dediquem-se e se esforcem em promover a segurança da informação e comunicações nas atividades que lhe são afetas, há outras, abertas e vulneráveis. Os protocolos, arquivos, intranet, internet, controles e política de acessos, telefone, fax etc. são canais desguarnecidos no que tange à Segurança de Informação e Comunicações em boa parte da APF (Relatório de Levantamento TC n.º 000.390/2010 TCU). As recomendações dos órgãos fiscalizadores da APF (Acórdão n.º 1603/2008 – TCU), que tem gasto boa parte de tempo em suas inspeções e recomendações quanto à segurança, mostram que, diferentemente da iniciativa privada, a APF não tem dedicada atenção devida a essa questão.

2.3. Metodologia

Este trabalho é composto por seis capítulos. Os dois primeiros são dedicados a exploração bibliográfica, exploratória, descritiva, qualitativa e analítica que se aplicam a segurança da informação. Procurou-se também levantar as principais discussões envolvendo a segurança da informação e conhecer a política de investimentos público em tecnologia da informação e as normas e regulamentações existentes para o setor. O capitulo três e quatro abordam aspectos da segurança e a terceirização, respectivamente. No capitulo quinto é feita breve discussão sobre o tema e a monografia finaliza no capitulo seis, com conclusões e trabalhos futuros.

3. Segurança

Este capítulo define alguns conceitos de segurança da informação e comunicações. Aborda também a questão do controle de acervo documental e apresentamos breves comentários sobre controle de acesso.

3.1. A Segurança da Informação

Segundo a norma ISO/IEC 17799:2000, segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos. Vulnerabilidade é considerada uma falha que expõe um sistema sob algum dos aspectos da segurança. Uma vulnerabilidade pode comprometer um sistema, como um todo ou parte dele, tornando-se um risco em potencial. A vulnerabilidade na computação significa ter brecha em um sistema computacional, também conhecida como *bug*.

Ainda segundo a ISO/IEC 17799:2000, a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade.

- Confidencialidade - Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- Integridade - O conceito de integridade está associado ao estado da informação no momento de sua geração e de seu resgate. Ela estará íntegra se em tempo de resgate estiver fiel ao estado original;
- Disponibilidade - Garantia de que os usuários autorizados tenham acesso à informação e aos sistemas correspondentes sempre que necessitarem deles.

A informação é mais um dos recursos a ser administrado pela organização. Neste sentido, aborda-se a seguir aspectos relevantes sobre a informação e seu valor para as organizações

O sistema de segurança da informação deve proteger as informações da empresa dos diversos tipos de ameaças, garantir a continuidade dos negócios, minimizar as perdas e maximizar o retorno dos investimentos e as oportunidades de negócios. (NBR ISO/IEC 17799:2005).

De acordo com Araujo (2005), todo tipo de documento de uma corporação deve exibir, de maneira clara, o respectivo grau de acesso, ou seja, seu grau de sigilo, o que requer classificar todas as informações segundo o seu grau de criticidade e âmbito de acesso:

- Informações Confidenciais: só podem ser disseminadas para empregados previamente nomeados. Na Administração Pública Federal temos o Decreto 4553, de 27 de dezembro 2002, que determina e normatiza os níveis de informações e como estes devem ser classificados. Por outro lado a segurança só terá sido alcançada se for observado além da classificação, o nível de acesso das pessoas autorizadas;
- Informações Corporativas: sua divulgação restringe-se ao âmbito da Empresa;
- Informações Públicas: podem ser disseminadas dentro e fora da Empresa.

A segurança da informação e comunicações jamais será alcançada se a tríplice PPT - Pessoas, Processos e Tecnologias – não for aplicada à estratégia de segurança. A figura 1 ilustra a forma tridimensional (uma variação) que a estratégia de segurança da informação deve ter para que seja efetiva.

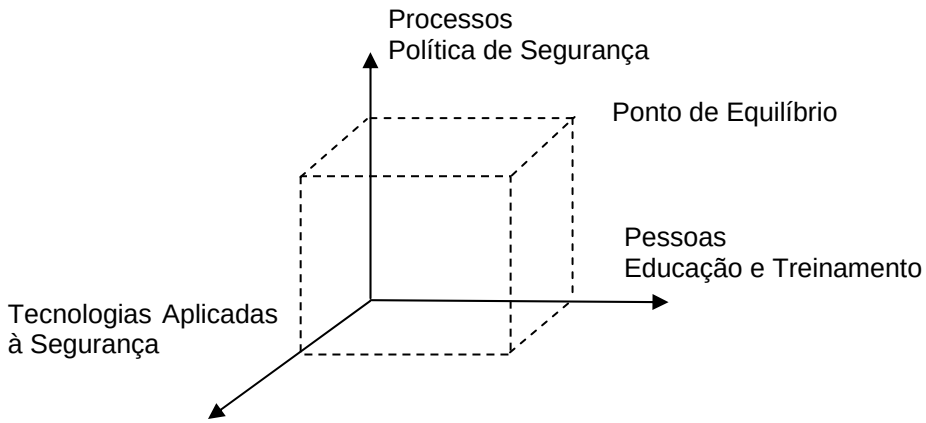

Figura 1. Pessoas, Processos e Tecnologias. Fonte: Voca, (2008).

O ponto de equilíbrio mostrado na figura 1 poderá ou deverá variar de empresa para empresa ou até mesmo de um processo de negócio para outro dentro da mesma empresa.

Explorando um pouco mais esta tríplice temos:

- Pessoas: educação – o que fazer; treinamento – como fazer e conscientização – por que fazer. As pessoas são o elo mais fraco da corrente da segurança.
- Processos: os processos devem ser flexíveis para dar agilidade e dinâmica à empresa, mas só até o ponto em que não afete a segurança da informação e comunicações. A partir daí devem ser tratados de forma rígida e metódica.
- Tecnologias: a tecnologia só deverá ser aplicada onde puder suportar a Política de Segurança da Informação, as Normas e os Processos definidos para cumprimento da estratégia de segurança, e para reforçar o elo mais fraco da corrente, as pessoas. Se a norma diz que a estação de trabalho deve ser bloqueada na ausência do usuário, aplica-se a tecnologia para que o bloqueio seja automático em caso de falha humana.

Qualquer estratégia de segurança que não complete esta tríplice, não assegurará o nível necessário de segurança da informação e comunicações, assim como a dosagem errada de cada parte também não o fará. Espera-se que a informação armazenada em um sistema computacional permaneça lá, com seu conteúdo intacto, ou seja, é expectativa de qualquer usuário que as informações estejam em local adequado, disponíveis no momento desejado, que sejam confiáveis, corretas e permaneçam protegidas contra acessos indesejados. Essas expectativas correspondem aos objetivos da segurança.

Entre os objetivos da segurança da informação e comunicações, Araujo (2005), destaca-se:

- Confidencialidade ou privacidade: proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação. Este objetivo envolve medidas como controle de acesso e criptografia.
- Integridade dos dados: evitar que dados sejam apagados, ou alterados sem a permissão do gestor da informação.
- Legalidade: estado legal da informação, em conformidade com os preceitos da legislação em vigor.

- Disponibilidade: garantir o provimento do serviço de informática, sob demanda, sempre que necessário aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicações de equipamentos/sistemas e backup. Um bom exemplo de ataque contra disponibilidade é a sobrecarga provocada por usuários ao enviar enormes quantidades de solicitação de conexão com o intuito de provocar pane nos sistemas.
- Consistência: certificar-se de que o sistema atua de acordo com a expectativa dos usuários.
- Isolamento ou uso legítimo: controlar o acesso ao sistema. Garantir que somente usuários autorizados possuam acesso ao sistema.
- Auditoria: proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e logs, que registram o que foi executado o sistema, por quem e quando.
- Confiabilidade: garantir que, mesmo em condições adversas, o sistema atuará conforme esperado. Antes de implementar um programa de segurança da informação e comunicações, é aconselhável responder às seguintes questões:

  a) O que proteger?

  b) Contra que ou quem?

  c) Quais as ameaças mais prováveis?

  d) Qual a importância de cada recurso?

  e) Qual o grau de proteção desejado?

  f) Quanto tempo, recursos humanos e financeiros se pretendem gastar para atingir os objetivos de segurança desejados?

  g) Quais as expectativas dos usuários e clientes em relação à segurança de informações?

  h) Quais as conseqüências para a instituição se seus sistemas e informações forem violados ou roubados?

As dificuldades em apontar responsáveis, levam as empresas a se dedicarem muitas vezes, em apenas corrigir falhas, porém, quando descobrem as causas, verificam que 24% das falhas são causadas pelos próprios funcionários e 20% por hackers, ou seja, problemas de origem humana; já os problemas com vírus 15%,

spam 10% e fraudes 8% são os que mais causam danos financeiros para as organizações, conforme mostra o Gráfico 1. (Módulo Technology for GRC. *Governance Risk and Compliance*. 10ª Pesquisa Nacional de Segurança da Informação. (2006).

Gráfico 1. Problemas que geraram perdas financeiras. Fonte: Módulo (2007).

Se as organizações atentassem para o fato de que suas perdas ou prejuízos são ocasionados por problemas na Segurança da Informação, implantariam com certeza imediatas medidas que minimizassem os problemas com segurança. No entanto, a maioria esmagadora das empresas ainda não percebe que a não conformidade com as normas específicas para área de segurança é uma das possíveis causas de prejuízos consideráveis. Muitas das empresas (75%) fazem algum tipo de terceirização na área de SIC, contra 25% que não o fazem. Quando a preferência é a terceirização, as companhias selecionam serviços como administração e suporte a firewall e IDS (16%), helpdesk (13%) e análise de riscos (9%), entregando dessa forma a estranhos a missão de zelar pela segurança, conforme demonstrado no gráfico 2.

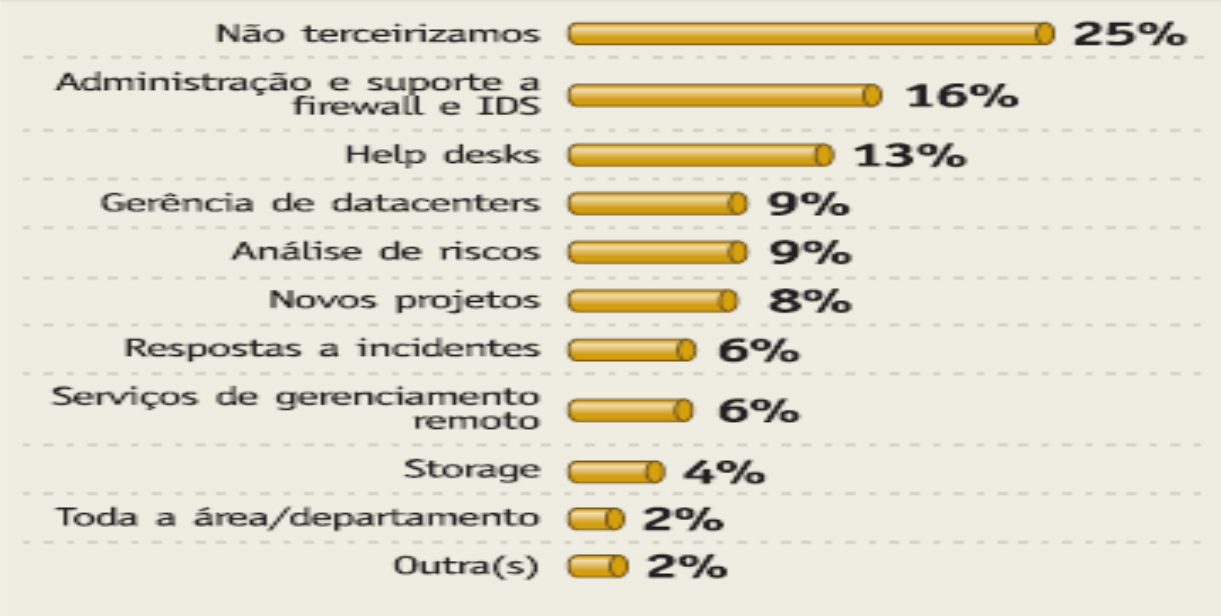

Gráfico 2. Área de segurança terceirizada. Fonte: Módulo (2007).

Para a maioria das empresas (55%), a falta de conscientização dos executivos e usuários é o principal obstáculo para a implementação de uma política da segurança. Seguindo a isto, ou em conseqüência disto, a falta de um orçamento adequado (Gráfico 3).

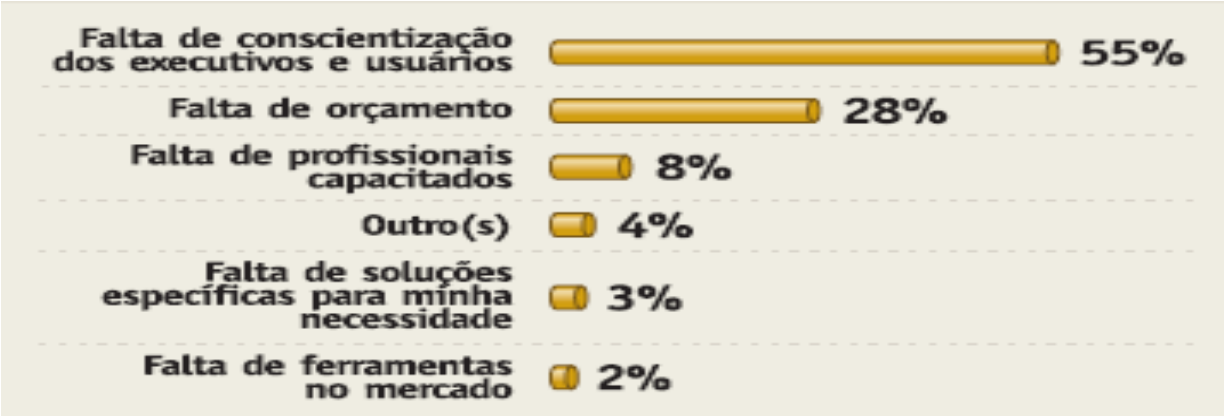

Gráfico 3. Principal obstáculo para a implantação de política de Segurança da Informação. Fonte: Módulo (2007).

Na Administração Pública Federal normas foram elaboradas para contemplar as necessidades especificas do serviço público.

Conforme disposto no inciso II do art. 3º da Instrução Normativa n.º 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional, compete ao

Departamento de Segurança da Informação e Comunicações – (DSIC), estabelecer normas definindo os requisitos metodológicos para implantação da Gestão de Segurança da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

O TCU, por meio do Acórdão 2.023/2005, define uma Política de Segurança da Informação nos termos das orientações contidas no item 3 da NBR ISSO/IEC 17799:2001, que estabelece os princípios norteadores da gestão da informação no Ministério e que esteja integrada à visão, à missão, ao negócio e às metas institucionais, observando a regulamentação ou as recomendações por ventura feitas pelo Comitê Gestor de Segurança da Informação instituído pelo Decreto 3.505/2000, e pelo Gabinete de Segurança Institucional da Presidência da República, conforme Decreto 5.408, de 1º de abril de 2005.

Já o Acórdão 1.603/2008 do TCU, após constatar diversas falhas na condução da Segurança da Informação e Comunicações no âmbito dos Ministérios, Tribunais e Empresas Públicas, recomenda a implantação de planejamento estratégico para a área de TI.

3.2. Segurança dos Acervos Documentais

A legislação referente ao direito de acesso, às restrições de uso e aos graus de sigilo documental, estabelece que a instituição deve adotar, também, procedimentos padronizados que sistematizem os processos de produção, tramitação, uso e destinação dos documentos.

A fim de preservar a segurança dessas informações, as instituições adotam medidas para monitorar seu acervo. O controle do acesso pode ser feito por meio do cadastro dos usuários, pelo crachá de identificação, ou até mesmo pela restrição do espaço do acervo ao uso exclusivo dos funcionários.

A Câmara Técnica de Documentos Eletrônicos (2006, p.32) afirma que a instituição "*precisa limitar ou autorizar o acesso a documentos, por usuário e/ou grupos de usuários*", garantindo, no mínimo, as funções de restrição de acesso, a exibição dos documentos somente aos usuários autorizados e o uso ou a

intervenção nos documentos para usuários com autorização. Em dezembro de 2009, o Conselho Nacional de Arquivos – (CONARQ), cria um modelo de requisitos para sistemas informatizados de gestão arquivista de documentos, visando garantir a segurança da informação entre outras medidas. “O sistema de gestão arquivística precisa limitar ou autorizar o acesso a documentos por usuário e/ou grupos de usuários. O controle de acesso deve garantir, no mínimo, as seguintes funções: restrição de acesso aos documentos; exibição dos documentos criptografados ou não, e dos metadados somente aos usuários autorizados; uso e intervenção nos documentos somente pelos usuários autorizados. Os documentos também devem ser analisados com relação às precauções de segurança, ou seja, se são considerados ostensivos ou sigilosos. No caso de documentos sigilosos, existem regras, normas e legislação que estabelecem diferentes razões e graus de sigilo a serem atribuídos a cada documento além de definirem as autoridades competentes a fazê-lo”.

Segundo o Fórum do Patrimônio Documental (2006, p.8), “*a instituição deve registrar cada consulta de forma correta e objetiva, e esses registros devem ser guardados em local seguro e por um longo prazo, para que possam estar disponíveis e rapidamente recuperáveis a qualquer instante*”. No caso de perdas ou furtos, a adoção desta medida possibilita a identificação do usuário que utilizou a documentação e de quando ocorreu sua consulta.

A atividade arquivística deve sempre considerar, entre outros aspectos, o grau de sigilo da documentação em questão, qualquer que seja seu suporte. No meio digital, os níveis de acesso determinam esse grau de sigilo, estando em consonância com a legislação vigente (LUZ, 2008).

3.3. Controle de Acesso

O acesso aos documentos é abordado de forma a verificar a eficiência dos sistemas utilizados na instituição. O administrador, ou seja, o arquivista é quem define o acesso por usuários ou grupos de usuários, no caso de acervos documentais. Ele também deve verificar constantemente quem possui direito de

acesso, quais os níveis de segurança e quais as restrições de acesso, estando sempre em consonância com a legislação vigente.

Cardoso e Luz (2005) afirmam que ao se produzir e difundir as informações, sejam eletrônicas ou digitais, compete aos profissionais estar constantemente atualizados para empregar ações inovadoras no tratamento dos documentos.

O emprego de um sistema de gestão leva tempo, requer dedicação e envolve uma série de procedimentos que, postos em prática, facilitam a busca à informação. A aplicação de um sistema de gestão de arquivos eletrônicos é mais complexa devido à falta de instrumentos que orientem sua aplicação.

A Norma ISO 15489, propõe a existência de controles de acesso apropriados, garantindo meio para o acesso. Os documentos de arquivo são divididos por categorias, de acordo com a gama de acesso em um determinado momento, e as pessoas devem ter permissão para acessá-los. Nesse sentido, Castro et al. (2007, p.23) colocam que, além dos requisitos já identificados, essa Norma ainda contempla “sugestões e requisitos que os arquivistas podem utilizar: cooperação com outros profissionais da informação, boas práticas de gestão necessárias para a produção e preservação de documentos de arquivo com qualidade”.

As políticas atualmente adotadas nas instituições para controlar o acesso, tanto do APERS – Arquivo Público do Estado do Rio Grande do Sul, (Agência Estadual da Tecnologia da Informação, 2008), quanto do AHPAMV – Arquivo Histórico de Porto Alegre – Moyses Velhinho são suficientes para garantir a segurança das informações, uma vez que, segundo pesquisa realizada pelo professor Daniel Flores e Josiane Ayres Sfreddo, publicado (Perspect. Cienc. Inf. Vol.14 n.º 2 – Belo Horizonte 2009) com o titulo: O controle de acesso na percepção dos profissionais de arquivo: Uma questão de segurança das informações institucionais, não há registros de problemas maiores como roubo ou perda de informação. Ainda assim, na opinião dos técnicos de arquivo, é interessante que seja instalado um sistema de segurança patrimonial para evitar possíveis roubos e haver maior controle na movimentação do acervo.

Uma instituição, para se defender de possíveis ameaças que comprometam a segurança da informação e comunicações, deve, além de criar políticas de segurança institucional, verificar quem possui acesso às informações sensíveis, ou

seja, informações de acesso restrito e, além disso, proteger documentos que estejam em sistemas eletrônicos. Para salvaguardar estas informações é necessário, ainda, o uso de Normalização para a segurança das informações.

Uma das preocupações, ao se estudar o controle de acesso e, principalmente, quando o referencial teórico são as Normalizações Arquivísticas, é a observância da legislação em vigor, quando se refere à documentação, principalmente em instituições públicas. O Conselho Nacional de Arquivos (2008, p. 44), no Decreto n.º 4.553, de 27 de dezembro de 2002, art. 2º, afirma que: “São considerados originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas”.

Para monitorar a movimentação de pessoas, as instituições adotam, ainda, regras internas que controlam o acesso aos documentos. Essas regras definem-se como condições de acesso impostas de acordo com as atividades, funções e necessidades de cada instituição. São regras como restrição de acesso ao espaço de guarda do acervo apenas a funcionários. Podem ser também regras de conduta do usuário/pesquisador visando orientá-lo sobre as mesmas, para que a consulta ao documento seja segura e o manuseio não danifique o acervo documental, sob guarda da instituição.

A supervisão e o planejamento das permissões do usuário e das responsabilidades de trabalho representam um processo realizado em todos os sistemas da gerência de documentos do arquivo, independentemente do seu formato (*International Organization for Standardization* ISO, 2001). As questões técnicas de controle do acervo e de acesso aos documentos devem ser planejadas, objetivando disponibilizar as informações aos usuários, sem que ocorram perdas e extravios de documentos. Neste sentido, a instituição deve registrar cada consulta de forma correta e objetiva, e estes registros devem ser guardados em local seguro e por um longo prazo, para que possam estar disponíveis e rapidamente recuperáveis a qualquer instante. Esta atitude permite que quaisquer perdas, danos ou roubos possam ser detectados, rapidamente identificado quem utilizou o acervo e quando (Fórum do Patrimônio Documental, 2006, p.6).

3.4. Vulnerabilidades

As ameaças, eventos ou atitude indesejáveis e que pode remover, desabilitar, danificar ou destruir um recurso, sempre existirão e estão relacionadas a causas que raramente as empresas controlam. Podem ter causas naturais ou humanas; causas internas ou externas. Dessa forma, entende-se que um dos objetivos da segurança da informação e comunicações é impedir que as ameaças explorem as vulnerabilidades e afetem um dos princípios básicos da segurança da informação (disponibilidade, integridade, confidencialidade e autenticidade) provocando danos ao negócio das empresas.

As ameaças são muitas das vezes conseqüências das vulnerabilidades existentes, provocando assim, perdas de disponibilidade, integridade confidencialidade e autenticidade. E podem ser divididas em:

- Ameaças naturais: fenômenos da natureza.
- Ameaças involuntárias: ocorre mais devido o desconhecimento, acidentes, ou erros, dentre outros.
- Ameaças voluntárias: Causadas por invasões, espiões, disseminadores de vírus de computador. São ameaças propositais e de origem humana.

As vulnerabilidades são frutos também de ameaças generalizadas e exploradas afetando assim a segurança das informações. As vulnerabilidades podem ser de acordo com Sêmola (2003 p.48-49):

- Físicas: salas de CPD mal planejadas, estrutura de segurança fora dos padrões exigidos.
- Naturais: computadores são propensos a sofrerem danos naturais, como tempestades, incêndio, além, por exemplo, de falta de energia, acúmulo de poeira, aumento da umidade e temperatura.
- Hardware: desgaste do equipamento, obsolescência ou má utilização.
- Software: má instalação, erros de configuração, vazamento de informações dependendo do caso, perda de dados ou indisponibilidade de recursos.

- Mídias: disquetes, CDs podem ser perdidos ou danificados, onde a radiação eletromagnética pode causar danos às vezes irreparáveis nas mídias.
- Comunicação: acessos não autorizados ou perda de comunicação.
- Humanas: vulnerabilidades referindo-se ao fator humano, como falta de treinamento, conscientização e o não seguimento das políticas de segurança.

4. Terceirização

A palavra “Terceirização” é oriunda da Ciência da Administração e foi adotada sem ajuste cientifico pelo Direito. A expressão deriva da palavra “terceira”, que para o interesse da administração se aplica na medida em que corresponde a delegação de execução de atividades acessórias a terceiros.

Muitas empresas buscam a terceirização com o objetivo de conquistarem redução de custos, gestão estratégica na área de compras, aumento do volume de contratos, redução do tempo de aprovisionamento de compras (*Lead time*), incorporação de visão estratégica, satisfação do cliente interno, melhoria contínua dos processos e redução da base de fornecedores.

O crescente aumento das ameaças ao ambiente tecnológico exige que as organizações desenvolvam processos cada vez mais eficientes para manter as informações seguras.

Quanto maior a prioridade dada à Segurança da Informação pela alta administração nas organizações, mais se observa o envolvimento e comprometimento do quadro de seus funcionários. A falta de conscientização dos gestores, por outro lado, é considerada um dos principais obstáculos para a implementação de políticas de segurança na maioria das organizações.

O Governo Federal vem buscando aumentar o número de contratações de funcionários públicos, através de concurso, em substituição aos terceirizados.

Não obstante, verifica-se que a preocupação com a Segurança da Informação e Comunicações nem sempre tem sido observada. A dispensa em massa de terceirizados gera riscos à continuidade do negócio, ao mesmo tempo em que se perde boa parte das informações, a *expertise* e a própria historia de alguns órgãos da APF.

Nos últimos dois anos, seguramente mais de 5.000 servidores terceirizados deixaram suas tarefas no serviço público dando lugar a servidores concursados. Do ponto de vista da legalidade da substituição não resiste nenhuma argumentação. Contudo, do ponto de vista da segurança da informação e comunicações,

consideramos que o risco foi gerado. O restante deste capítulo aborda o processo de terceirização e suas características.

4.1. O processo de terceirização

À medida que as demandas na gestão do processo de compras, por exemplo, se tornam mais freqüentes nas grandes corporações, o caminho natural é terceirizar as responsabilidades. A terceirização, *(outsourcing)*, consiste na contratação de terceiros para prestação de serviços ou fornecimento de produtos visando diminuir a estrutura operacional da empresa. De acordo com Ferreira (1998), a terceirização permite à empresa centralizar sua atenção na atividade fim, deixando as atividades meio para os terceiros. Desta forma, pode canalizar esforços para o aumento da qualidade, competitividade e produtividade, tornando-a mais leve e ágil. Hoje, por exemplo, uma empresa de telecomunicações não precisa despender esforços para comprar um bebedouro nem se preocupar com pequenos serviços e reparos do cotidiano. Tem, sim, de direcionar a atenção de seus profissionais de compras para a aquisição de produtos diretos, relacionados ao core business, como equipamentos e componentes de telecom.

Segundo o que afirma Carlos Roberto Caetano em seu artigo com o titulo: “a Terceirização através da utilização das centrais de compras”, publicada na revista TecHoje, têm-se dado grande ênfase à otimização e ao aumento da eficiência de todo o fluxo de materiais dentro da empresa e na cadeia de suprimento. A logística está em evidência e a estratégia é o uso efetivo dos recursos de comunicação e da tecnologia de informação, que são a principal força motriz na busca de melhorias de lucratividade no campo da logística.

Segundo Martins (2005), para obter resultados efetivos, é necessário que a empresa escolha um fornecedor de serviços de *outsourcing* que incorpore as melhores práticas de mercado e tecnologias acessíveis. É vital que a empresa analise quais categorias devem ser terceirizadas, bem como definam as *SLAs* (*Service Level Agreement*) que devem ser implementadas para atender às necessidades estratégicas corporativas. O grande diferencial para as organizações

que optam pela terceirização é a aplicação dos níveis de serviços agregados. Martins (2005).

Segundo Gaona (1995), para uma empresa colher dividendos que ultrapassem sua eficiência operacional, é imperativo que a alta gerência encare a terceirização de maneira estratégica, e não como uma decisão operacional. Para Ravi Aron, professor de administração de operações e de informações da Wharton, executivos de alto escalão que tratam a terceirização basicamente como uma manobra que permite cortar custos não se preocupam, de modo geral, em implementar modificações organizacionais de peso. Contudo, é isso o que normalmente se requer para que a terceirização produza benefícios estratégicos.

A terceirização é a formulação clássica expressa pelo binômio fazer x comprar. Devo produzir internamente determinado bem ou adquiri-lo no mercado? E como posso agregar valor de modo mais eficaz? Essa é uma questão que vem sendo estudada há décadas pela economia e pela administração. Não se trata, portanto, de problema novo, nem é tampouco algo que um dia não nos incomodará mais. O que mudou é que o número de empresas que hoje terceirizam é maior do que nunca e usando, para isso, expedientes até então inéditos.

Hoje em dia, a terceirização ganhou dimensões que as empresas, há dez anos, jamais poderiam imaginar. Não é mais apenas uma opção tática que permite às empresas economizar recursos financeiros. Antes, tornou-se uma necessidade estratégica em uma era em que são inúmeras as oportunidades oferecidas por “países de custo baixo”, como a China, a Índia e o México. Na verdade, a terceirização seguirá adiante transformando as economias dos países desenvolvidos e emergentes.

4.2. Vantagens da Terceirização

Para Morris Cohen, professor de fabricação e logística da Wharton – EUA, em artigo publicado na revista Gestão das Operações (2004), diz: **“**a terceirização traz consigo algumas vantagens estratégicas como o conhecimento tecnológico, o acesso a processos ou capacidades melhores e o aprendizado de procedimentos de gestão mais eficientes. Com a terceirização, se ganha acesso a um conhecimento e

a uma capacidade superiores. Existem companhias que também terceirizam capacidades. Elas sabem como fazer um determinado produto, mas não dispõem de capacidade para produzi-lo, ou simplesmente não querem investir na tecnologia necessária à sua fabricação".

Segundo Gaona (1995), a terceirização, proporciona instrumentos de gestão capazes de melhorar o desempenho das organizações, como: criação de vantagem competitiva pela criação de novas empresas, oferta de mão-de-obra diferenciada, oferta de empregos, especialização, aumento da competitividade, melhoria e controle da qualidade, aprimoramento do sistema de custeio, treinamento e aprimoramento, diminuição do desperdício como ponto fundamental, otimização dos recursos, valorização de talentos humanos, agilidade de decisões e menor custo.

Para Fleury (1999), dentre as inúmeras vantagens da terceirização, pode-se citar o acesso a novos recursos tecnológicos, a agilidade na implementação de novas soluções, a previsibilidade dos gastos/custos e prazos, o aumento de especialização, a liberação da criatividade, o acesso ao pessoal qualificado, o crescimento do mercado regional e a mudança na cultura interna da empresa.

4.3. Riscos na Terceirização

A terceirização envolve riscos que não devem ser descartados: cadeias de fornecedores mais longas, incerteza política, possíveis dificuldades no monitoramento das operações dos fornecedores, além de questões de cunho lingüístico e cultural. Algumas empresas americanas reduziram ou eliminaram a terceirização de *call centers* para a Índia por causa de dificuldades culturais e de queixas de clientes. Há também o risco de que um fornecedor se torne concorrente da empresa. A Acer, por exemplo, fundada em Taiwan em 1976, era, no início, fornecedora de componentes para micro computadores; contudo, com o passar do tempo, tornou-se uma das principais fabricantes de computadores do mundo.

Nem sempre o custo total será menor, quando se achar alguém que faça algo por um preço inferior. Quem tem uma longa cadeia de suprimentos não deve esperar que seu custo seja menor do que aquele que tem uma cadeia mais curta. Por outro lado, segundo Harold Sirkin (Estratégia 2005), vice-presidente sênior e

diretor do escritório da BCG de Chicago, e também chefe de práticas operacionais globais da empresa, pode ser catastrófico para uma empresa evitar a terceirização por causa de uma aversão irracional a riscos. Os riscos associados à inércia e à relutância em relação à mudança podem deixar a empresa em desvantagem absoluta no tocante a concorrentes mais dinâmicos e dispostos a correr riscos.

Há uma avaliação equivocada quando se fala em risco. Há riscos visíveis e invisíveis. Quando uma empresa se dispõe a arcar com custos desvantajosos, ou quando se obriga a investir mais do que deveria em processos de fabricação, incorre em riscos fabulosos, mas que são difíceis de perceber.

Segundo Jon Gossels, presidente da consultoria *SystemExperts*, quando se trata de terceirizar funções de segurança, o ceticismo ainda toma conta de muitos usuários. É, no mínimo, controversa a idéia de delegar o controle da segurança da rede a uma empresa paga para manter o equipamento, monitorar ataques, fazer varreduras, coletar registros ou atualizar *software* de segurança para os funcionários. Muitos gerentes de segurança temem que, com a terceirização, os riscos à segurança passem despercebidos porque o pessoal de fora obedecerá a um contrato mecanicamente, sem uma atenção mais criteriosa.

Ultimamente, percebe-se que a terceirização apresenta também um outro lado da moeda: a falta de identidade com a empresa e funcionários não preocupados com a qualidades dos serviços e com a satisfação do cliente. Algumas empresas estão trazendo de volta para o corpo de funcionário, os serviços terceirizados, principalmente as do ramo automobilístico no ABC paulista. Nos últimos quinze anos, a terceirização tem sido apontada como uma das maiores inovações organizacionais. Inúmeras empresas brasileiras – pressionadas pela necessidade de redução de custos, em face da abertura econômica – passaram a se concentrar nas suas atividades principais e buscaram terceirizar tudo o mais que fosse possível. Na teoria, enfatizam-se os ganhos da especialização e da cooperação entre empresas. Consultores apontam o *outsourcing* como o caminho para a modernidade e a vantagem que a terceirização traz na transformação de gastos fixos em variáveis: se o faturamento cresce, compra-se mais o serviço; se o faturamento cai, reduzem-se os pedidos do serviço terceirizado, com a ausência de rescisões contratuais e multas trabalhistas.

O modismo não se limitou ao setor privado. “Prefeitura terceiriza zona azul”, “Governo paulista quer terceirizar parques”, “Secretário propõe terceirizar o Detran”, “Brasil já tem prisões com administração terceirizada”, “Cobrança da dívida ativa poderá ser terceirizada no município”, “Estado inaugura hospitais terceirizados” – são apenas alguns dos vários títulos de notícias envolvendo a terceirização no setor público.

O procurador do Trabalho, Helder Santos Amorim, em seu livro intitulado “Terceirização no Serviço Público – Uma análise à luz da nova hermenêutica constitucional”, diz: “No plano institucional, a terceirização dinamiza o movimento de desregulamentação institucional e de desprofissionalização do serviço público, liquidando funções e esgotando planos de carreiras indispensáveis ao exercício das responsabilidades estatais. No plano social, a terceirização no serviço público enseja a precarização das condições de trabalho, a fragilização da organização coletiva dos trabalhadores e a discriminação entre servidores públicos e terceirizados. A superterceirização coloca o Estado na rota da exploração desmedida da mão-de-obra privada flutuante, sob o mesmo regime de controle quantitativo que move a iniciativa privada na busca pelo absoluto domínio do capital sobre o trabalho, ao passo que seus próprios servidores, envolvidos nas mesmas atividades de finalidade social, gozam de maior segurança jurídica e social”. (Fonte: *Procuradoria-Regional do Trabalho da 3ª Região).*

Na prática, as terceirizações ultrapassaram rapidamente as atividades tradicionais de e alcançaram as áreas estratégicas nas diferentes empresas. Nos bancos, a terceirização atingiu a compensação de cheques e os caixas de atendimento; na indústria automobilística, a montagem de pneus, a pintura e a ferramentaria; no comércio, o trabalho dos caixas de supermercados; nos hospitais, setores como o laboratório clínico. Essa invasão da atividade-fim se deu em praticamente todos os ramos e setores.

Segundo Motta (2007), secretária nacional de organização da Central Única dos Trabalhadores - CUT são muitos os acidentes de trabalho envolvendo terceirizados sem experiência e sem treinamento na extração de petróleo e em serviços relacionados à geração e distribuição de energia. Lotes de cheques são extraviados e cadastros dos clientes são repassados indevidamente sem que os

bancos queiram assumir suas responsabilidades, alegando que o problema aconteceu com “terceiros”.

A décima edição da Pesquisa Nacional de Segurança (2007) da Informação traz uma visão atualizada sobre as tendências do mercado brasileiro, com seus indicadores e melhores práticas, na qual os órgãos do Governo participam com 21% de representatividade. Pela primeira vez, a Pesquisa Nacional de Segurança da Informação e Comunicações, aborda temas como: a condução de análise de riscos nas organizações, capacitação de equipes e a conscientização de funcionários.

A evolução do mercado de tecnologia e a maior conscientização sobre a necessidade de investimentos em SIC ajudaram as empresas a estarem mais preparadas para enfrentar algumas falhas de segurança. No entanto, ainda é grande o número de companhias (33%) que não sabem quantificar as perdas ou sequer identificar os responsáveis pelo problema (21%). Os órgãos públicos são os que menos sabem informar sobre a quantificação dos prejuízos oriundos das falhas na segurança.

Segundo a Modulo Technology for GRC. *Governance Risk and Compliance*. (10ª Pesquisa Nacional de Segurança da Informação) (2006), ainda é considerável o número de companhias (19%) que não têm departamento de segurança da informação e que terceirizam as ações pontualmente. A área de governo é o que tem mais órgãos onde a segurança da informação está ligada à estrutura da alta administração do órgão. (14%) (Tabela 4).

	(porcentagem por segmento)
Comércio	0%
Financeiro	10%
Governo	14%
Indústria	0%
Serviços	10%
Telecom	13%

Tabela 4. Setores em que o departamento de segurança da informação e comunicações está ligado à presidência. Fonte: Módulo (2007).

Também segundo a (Modulo Technology for GRC. *Governance Risk and Compliance*. 10ª Pesquisa Nacional de Segurança da Informação. (2006), todos os setores consideram os profissionais que lidam com a Segurança da Informação nas organizações, parcialmente capacitados. No entanto, praticamente só Governo e Comércio estavam em fase de planejamento e de investimentos em capacitação de seus quadros. (Tabela 5). Contudo, essa realidade está mudando. O governo através do GSI/DSIC/PR, várias ações na direção de criação de políticas próprias adequadas a cada órgão da Administração Pública Federal. Prova disso é a publicação da Instrução Normativa GSI n.º 1, de 13 de julho de 2008. Além da IN/GSI/01, se seguiram as Normas Complementares 01 a 08, esta última publicada em agosto de 2010.

Comércio	48%
Financeiro	13%
Governo	40%
Indústria	29%
Serviços	42%
Telecom	45%

Tabela 5. Setores que não possuem planej. formal de segurança. Fonte: Módulo (2007).

Segundo a Modulo Technology for GRC. *Governance Risk and Compliance*. (10ª Pesquisa Nacional de Segurança da Informação) (2006), demonstrada na tabela 6, observa-se que o Governo é setor onde a maioria de seus funcionários não tem conscientização adequada quanto a importância da Segurança da Informação.

Está realidade está mudada, considerando o grande esforço feito pelo GSIPR nos últimos anos, na criação de política de segurança em cada órgão da Administração Publica Federal (APF). Soma-se a isso, o nível de conscientização e treinamentos que os servidores públicos têm recebido sobre a necessidade de aperfeiçoamento da segurança da informação nos órgãos.

Comércio	38%
Financeiro	61%
Governo	29%
Indústria	44%
Serviços	50%
Telecom	33%

Tabela 6. Setores em que as campanhas de sensibilização são preparadas pelas áreas de Seg. da Informação e Comunicações, Marketing e RH. Fonte: Módulo (2007).

4.4. O Fator Humano

Muitas organizações ignoram as questões sociais e comportamentais em seus programas de segurança da informação e comunicações. É um erro imaginar que os aspectos humanos sejam menos importantes, e que o estabelecimento de políticas e a aplicação de controles técnicos sejam suficientes para garantir um ambiente seguro.

As políticas de segurança da informação e comunicações são apresentadas na forma de guia de conduta no qual os usuários dos sistemas de informação devem se adequar integralmente (Marciano & Lima Marques, 2006). Para que essas políticas sejam efetivamente legítimas e que as pessoas as incorporem nas suas atividades do dia-a-dia é necessário o envolvimento e a participação de toda a comunidade de usuários desde o início do processo de discussão e elaboração das mesmas.

De acordo com o artigo 1º do Decreto 2.271/1997, a terceirização é permitida nas áreas de conservação, limpeza, segurança, vigilância, transportes, informática, copeiragem, recepção, reprografia, telecomunicações e manutenção de prédios, equipamentos e instalações. Nesse mesmo sentido o acórdão n.º 1.603/2008 do (TCU), recomenda medidas para a área de TI, após ter constatado a deficiência da estrutura de pessoal, tratamento da confidencialidade integridade e disponibilidade das informações. Atualmente grande parte da Administração Publica Federal (APF), desenvolve ações para minimizar o problema da segurança da informação. Na área de TI, por exemplo, as fabricas de software são contratadas apenas para o desenvolvimento, ficando a cargo do órgão público o controle da segurança.

O fator humano tem se mostrado um dos grandes riscos para a Segurança da Informação. Após essa constatação, os cuidados com a terceirização, por exemplo, tem sido fator de preocupação pelos gestores públicos. A máxima de que “não há corrente mais forte do que seu elo mais fraco” é evidente quando o uso indiscriminado de terceirização se dá em setores com grande implicação na segurança da informação.

5. Discussão

Os capítulos anteriores desta monografia apresentaram definições e conceitos relacionados à segurança da informação e comunicações, indicando a necessidade de preocupação com segurança tanto no que se refere aos acervos de informação manipulados nos ambientes de tecnologia da informação, como nos acervos de documentos mantidos nos arquivos públicos. Tomando por base os conceitos de segurança da informação, o trabalho apresentou as características, vantagens e riscos da terceirização, em sua relação com a segurança da informação e a continuidade dos serviços em órgãos públicos nos quais há um elevado contingente de terceirizados. A fim de que as características perniciosas do processo de terceirização e de desterceirização seja melhor abordadas sob o ponto de vista da segurança o autor destacar o papel central desempenhado por uma política de segurança.

A definição da política de segurança é o primeiro passo para o reconhecimento da importância da segurança da informação e comunicações para a organização e para seu tratamento adequado. A ausência da política de SIC é o indício de que a gestão da segurança da informação e comunicações é inexistente ou incipiente no órgão. Não se pode, entretanto, alegar falta de regulamentação na administração pública federal do Brasil. O setor público conta com uma série de instrumentos regulatórios relacionados com a segurança da informação e comunicações endereçada a seus órgãos e entidades.

Recentemente o Ministério do Trabalho e Emprego, publicou a Portaria Ministerial n.º 1327 de 11 de junho de 2010, aprovando a Política de Segurança da Informação e Comunicações – (POSIC do MTE).

Isto revela a atenção que o assunto vem merecendo por parte dos gestores no que tange o cumprimento das normas e orientações dos órgãos de controle, não só como resposta às determinações, mas também pelo entendimento de que todos os esforços devem ser envidados na salvaguarda de seus ativos. Esta preocupação, no entanto, não aborda características e condicionantes dos processos de terceirização e desterceirização.

Uma política de informação adequada deve contemplar adequadamente a todas as fases do ciclo de vida de uma informação, que vai desde a sua criação, classificação, publicação ou divulgação e até a sua definitiva exclusão. Mas isso exige responsabilidade, capacidade e comprometimento do gestor. Nesses aspectos, a excessiva terceirização do Estado cria lacunas inaceitáveis que comprometem e minam a soberania do país, tanto em seus aspectos sociais como econômicos.

O grau de segurança das informações e comunicações de uma instituição está diretamente relacionado ao nível de conscientização e treinamento de seus membros quanto as suas responsabilidades em preservar a segurança física e lógica da organização. Cada colaborador deve ter pleno conhecimento do que se espera de suas responsabilidades. Medidas de segurança devem ser utilizadas e as sanções previstas em caso de violação das mesmas. Para isto, é necessário que haja normas e procedimentos claros, a serem seguidos por todos. O treinamento e conscientização encorajam os colaboradores a identificar e a reportar as possíveis falhas que impliquem na violação da segurança.

O Governo Federal vem buscando implantar um programa de "desterceirização" no setor público. Neste sentido, foi firmado, entre o Tribunal de Contas da União e o Poder Executivo da União, acordo de desterceirização (Termo de Conciliação Judicial – Processo nº 00810-2006-017-10-00-7), estabelecendo que até o final de 2010 um total de 33.000 trabalhadores temporários, considerados irregulares pelo Tribunal de Contas da União, serão substituídos por servidores aprovados em concurso público.

Um dos objetivos deste trabalho foi o de esclarecer as características gerais do processo de terceirização e desterceirização, visando torná-lo mais efetivo sob o ponto de vista da segurança.

É nesse ponto que concluí-se esta discussão, reconhecendo, que os esforços que a Administração Pública Federal vem implementando na difusão da cultura de SIC, ensejados pelas recomendações dos órgãos de controles, tem produzido bons resultados. Contudo, dada complexidade e pluralidade de ações desenvolvida pela APF, entende-se que a criação de núcleos de gestores de Segurança da Informação e Comunicações, atuando especificamente na implantação de políticas de segurança da informação, e com plena consciência das características do processo

de terceirização imprimiria maior velocidade na disseminação e aprimoramento da cultura de SIC.

6. Conclusões e Trabalhos Futuros

Este trabalho originou-se da preocupação do autor com o processo de terceirização e em seguida o processo de desterceirização em órgãos da administração pública federal, na sua relação com a segurança da informação.

O objetivo geral do trabalho foi analisar a expansão do processo de terceirização, como fator de risco à segurança da informação e comunicações no serviço público no Brasil. Por meio de discussões e reflexões embasadas em bibliografia sobre o assunto ficou demonstrado que o fator humano, sendo um dos principais elementos relacionados a segurança da informação, é fortemente afetado pelos fenômenos da terceirização e desterceirização, tão freqüentes no serviço público.

Neste sentido, o autor propõe que as discussões sobre terceirização sejam melhor abordadas na formulação de políticas de segurança, especialmente na atuação dos gestores de segurança da informação e comunicações.

Referências

ABNT, A.B. de N.T. Tecnologia da Informação – Código de pratica para gestão da segurança da informação: Nbr ISO/IEC 17799. Rio de Janeiro, 2000.

AMORIN, Helder Santos. Terceirização no Serviço Público ISBN 9788536113005 Ed.LTr

APERS, Arquivo Público do Estado do Rio Grande do Sul, (Agencia Estadual da Tecnologia da Informação, 2008)

ARAUJO, E. E. de, A Vulnerabilidade Humana na Segurança da Informação, 2005, http://www.si.uniminas.br/TFC/monografias/Monografia%20Final%20Eduardo %20Edson.pdf

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799:2005: Tecnologia da Informação: Técnicas de Segurança: Código de Práticas para Gestão da Segurança da Informação. Rio de Janeiro 2005.

BRASIL. Decreto n.º 3505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da administração pública. Diário Oficial 14 de junho de 2000, disponível no sitehttp://WWW.planalto.gov.br/ccivil_03/decreto/Quadros/2000.htm

BRASIL. Lei 9597 de 12 de novembro 1997

BRASIL, Decreto 2.271, de 7 de julho de 1997, DOU de 8/7/97.

BRASIL. Decreto 4553 de 27 de dezembro de 2002.

BRASIL, Decreto 5.408, de 1º de abril de 2005.

BRASIL, Tribunal de Contas da União (TCU), Relatório de Levantamento TC nº 000.390/2010.

BRASIL, Tribunal de Contas da União (TCU),Acórdão 2.023/2005

BRASIL, Tribunal de Contas da União (TCU),Acórdão 1.603/2008

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos: e-ARQ. Rio de Janeito: Conarq, 2006. Disponível em: <http://www.conarq.arquivonacional.gov.br /Media/publicacoes/ earqbrasilv1.pdf>. Acesso em: 26 jun. 2010.

CARDOSO, J.C.; LUZ, A.R. Os arquivos e os sistemas de gestão da Qualidade. Arquivística.net, Rio de Janeiro, v.1, n.1, p.51-64, jan./jun. 2005. Disponível em: <www.arquivistica.net/ojs/include/getdoc.php?id=51&article=6&mode=pdf>. Acesso em: 29 jun. 2010.

CASTRO, A.M.; CASTRO, A.M.; GASPARIN, D.M.C. Arquivos: físicos e digitais. Brasília: Thesaurus, 2007.

CIO BRASIL – Publicado em 28/12/09

CONSELHO NACIONAL DE ARQUIVOS. Decreto n. 4.553, de 27 de dezembro de 2002, Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Diário Oficial da União, 30 de dezembro de 2002. p.6.

CONSULTOR JURÍDICO - 10 de Maio de 2010, Município com pior IDH do país tem alto índice de cargos comissionados, Disponível em: http://www.jusbrasil. com.br/noticias/2180703/ municipio-com-pior-idh-do-pais-tem-alto-indice-de-cargos-comissionados. Acesso em: 12 jun. 2010

FERREIRA, F.R.N. Supply Chain Management: in Revista Evoluções e Tendências. Vitória: Faculdade de Ciências Humanas de Vitória, 1998.

FLEURY, P.F. Supply Chain Management: conceitos, oportunidades e desafios de implementação. Revista Tecnologística. São Paulo: Ano V, n.39, fev,1999.

FLORES, Daniel e SFREDDO, Josiane Ayres, (Perspect. Cienc. Inf. Vol.14 nº 2 – Belo Horizonte (2009).

FOLHA DE SÃO PAULO 08.09.2010

FÓRUM DO PATRIMÔNIO DOCUMENTAL. Grupo de trabalho de controle de 2010. acesso e circulação de acervo. Documento final. Rio de janeiro, julho 2006. Disponível em: <www.aab.org.br/download/GT_acervo25jul.pdf>. Acesso em: 13 jun.

GAONA, H.B.M. O Uso da Simulação para Avaliar Mudanças Organizacionais na Produção. Florianópolis. Dissertação de Mestrado. Programa de Pós-Graduação em Engenharia de Produção. Universidade Federal de Santa Catarina, 1995.

GOSSELS, Jon, (Presidente da Consultoria SystemExperts). Terceirização em segurança gera dúvidas em profissionais de TI. (25 de março 2008) Fonte: Computerworld.

HENRIQUES, C. ISO 15489-1 e ISO/TR 15489-2: uma Norma para gestão de arquivos. Lisboa: Instituto dos Arquivos Nacionais/Torre do Tombo, 2002. Disponível em: <www.dotecome.com/infoimagem/infoimagem/info38/38art3.htm - 15k>. Acesso em: 21 jun 2010.

HUEBNER, A.R.; BRITT, M. M. Analyzing Enterprise Security Using Social Networks and Structuration Theory; Journal of Applied Management and Entrepreneurship, Jul 2006; 11, 3; ABI/INFORM Global pg. 68.

IDC (IDC Brasil Conferencia 2009: TI e Telecom no Governo Brasileiro).

INSTRUÇÃO NORMATIVA, 01/IN01/DSIC/GSIPR, 13 de julho de 2008.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO 15489-1: International Standard – Information and documentation – Records management – Part 1: General. 2001. 26p.

LUZ, A.R.A.V. Normas Arquivísticas e Padrões de descrição de metadados aplicados à preservação do patrimônio arquivístico digital. 2008. Acesso em: 16 de mai. 2010.

MARCIANO, J.L.; LIMA MARQUES, M. O enfoque social da segurança da informação, Ci. Inf., Brasília, v. 35, n. 3, p. 89-98, Acesso em: 20 jun. 2010.

MARTINS, Sérgio Pinto. (2005). A Terceirização e o Direito do Trabalho. 7ª Edição

MINISTÉRIO DO PLANEJAMENTO E GESTÃO – Agosto/2000

MIINISTÉRIO DO TRABALHO E EMPREGO, Portaria Ministerial nº1327 de 11 de junho 2010.

MÓDULO - Décima da Pesquisa Nacional de Segurança, 2007, Disponível em http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf, Acesso em: 25 jun. 2010.

MORRIS, C.Sings, Languge end behavior. New York: Georg Braziller, 1964

MOTTA, D., MUNDO DO TRABALHO: Terceirização: modismo, mea-culpa e projeto, 2007, Disponível em http://www2.fpa.org.br/o-que-fazemos/editora/teoria-e-debate/edicoes-anteriores/mundo-do-trabalho-terceirizacao-modismo-mea, Acesso em: 27 jun. 2010.

O TRABUCO - Mantega: "contratação de 41 mil é desterceirização" ,2004, Disponível em http://www.otrabuco.com.br/lermais_materias.php?cd_materias=20476, Acesso em: 26 jun. 2010.

PORTAL R7 Publicado em 08/09/2010

RESOLUÇÃO, 20 Casa Civil, Arquivo Nacional, Conselho Nacional de Arquivos, 16 de julho de 2004.

REVISTA, Risk Report Ed.de 11 de agosto 2006 – Seção: Soluções – Gestão

SIRKIN, Harold, A Nova face da administração chinesa.Revista Estratégia, 20 de abril de 2004.

TERMO DE CONCILIAÇÃO JUDICIAL – Processo nº 00810-2006-017-10-00-7

VOCA - Vasques, Oliveira & Consultores Associados. As Tríplices da Segurança da Informação. Disponível em http://www.voca.com.br/TripliceSegInformacao.aspx, Acesso em: 28 jun. 2010

WIKIPEDIA. Information security, Wikipedia, The Free Encyclopedia, 24 de setembro de 2007, 12:38 UTC. Disponível em:<http://en.wikipedia.org/w/index.php?title=Information_security&oldid=160000515>. Acesso em: 29 jun. 2010

Apêndice A

TERMO DE CONCILIAÇÃO JUDICIAL - PROCESSO N° 00810-2006-017-10-00-7

O MINISTÉRIO PÚBLICO DO TRABALHO, *neste ato representado pela Procurador-Geral do Trabalho, Dr. Otávio Brito Lopes, e pêlos Procuradores do Trabalho, Dr. Fábio Leal Cardoso e Dra. Viviann Rodriguez Mattos, e a* ***UNIÃO,*** *neste ato representada pela Advocacia Geral da União, por meio do Advogado-Geral da União, Dr. José Antônio Dias Toffoli, e pelo Procurador-Geral da União, Dr. Luís Henrique Martins dos Anjos, e pelo Ministério do Planejamento, Orçamento e Gestão, por meio do Ministro de Estado do Planejamento, Orçamento e Gestão, Sr. Paulo Bernardo Silva, na forma do art. 5°, § 6°, da Lei n° 7.347, de 24 de julho de 1985, combinado com o art. 876 da Consolidação das Leis do Trabalho (Decreto-Lei n° 5.492, de 1 de maio de 1943),*

CONSIDERANDO *a existência da Ação Civil Pública n° 00810-2006-017-10-00-7, ajuizada pelo Ministério Público do Trabalho em face da UNIÃO, cujo objeto versa sobre a intermediação irregular de mão-de-obra praticada no âmbito da Administração Pública Federal Direta;*

CONSIDERANDO *que existem outras ações civis públicas ajuizadas e vários procedimentos investigatórios em diversas Procuradorias Regionais do Trabalho envolvendo o tema da terceirização imprópria em órgãos da Administração Pública Federal Direta;*

CONSIDERANDO *que o acesso a cargos e empregos públicos é condicionado à prévia aprovação em concurso público de provas ou de provas e títulos, conforme previsto no art. 37, II, da Constituição Federal;*

CONSIDERANDO *que o Enunciado n° 331, I, do Tribunal Superior do Trabalho, estabelece que a contratação de trabalhadores por meio de empresa interposta é ilegal, salvo nos casos previstos na Lei n° 6.019, de 3 de janeiro de 1974;*

CONSIDERANDO *que o Decreto n° 2.271, de 7 de julho de 1997, estabelece os parâmetros para a identificação dos serviços passíveis de terceirização no âmbito da Administração Pública Federal;*

CONSIDERANDO *que o Ministério do Planejamento, Orçamento e Gestão apresentou ao Tribunal de Contas da União proposta para substituir empregados terceirizados por servidores concursados, tal como ficou assentado no acórdão n° 1520/2006 - TCU;*

CONSIDERANDO *que a União vem sendo responsabilizada de forma subsidiária por créditos trabalhistas insatisfeitos de trabalhadores de empresas prestadoras de serviços, na forma da Súmula 331, IV, do Tribunal Superior do Trabalho;*

CONSIDERANDO *as reuniões preparatórias realizadas entre o Coordenador Nacional de Combate às Irregularidades Trabalhistas na Administração Pública e Assessores Técnicos do Ministério do Planejamento, Orçamento e Gestão, nas quais restou consolidado o entendimento de que a abrupta solução de continuidade na prestação de tais serviços terceirizados poderia gerar ofensa a bem jurídico de igual importância àquele tutelado na referida Ação Civil Pública;*

CONSIDERANDO *que, no âmbito do Poder Executivo Federal, a matéria de pessoal é da competência do Ministério do Planejamento, Orçamento e Gestão;*

CONSIDERANDO *a relevância e a obrigatoriedade de regularização de todos os contratos de prestação de serviços terceirizados,*

RESOLVEM CELEBRAR

TERMO DE CONCILIAÇÃO JUDICIAL,

nos seguintes termos e condições:

CLAUSULA PRIMEIRA. *A UNIÃO se compromete a contratar serviços terceirizados apenas e exclusivamente nas hipóteses autorizadas pelo Decreto n° 2.271, de 7 de junho de 1997, observado o disposto no artigo 37, inciso XXI, da Constituição Federal.*

Parágrafo *1° A responsabilidade pela contratação de serviços terceirizados em desacordo com o disposto no Decreto n° 2.271, de 7 de junho de 1997, será da autoridade competente para a assinatura do contrato e do respectivo ordenador de despesas, solidariamente.*

Parágrafo *2° O responsável pela assinatura dos contratos no âmbito de cada ministério, órgão ou entidade deverá identificar as atividades terceirizadas, o quantitativo total de terceirizados e a indicação das parcelas de recursos orçamentários que deixarão de ser disponibilizadas em decorrência da regularização gradativa das contratações conforme o cronograma e proporções estabelecidas na cláusula terceira deste termo.*

CLÁUSULA SEGUNDA. *A União se compromete a regularizar a situação jurídica dos seus recursos humanos, com a consequente rescisão dos contratos de prestação de serviços cujas atividades exercidas pêlos trabalhadores terceirizados não estejam de acordo com o disposto no Decreto n° 2.271, de 7 de junho de 1997.*

Parágrafo *1° Os órgãos da Administração Pública Federal deverão elaborar, em conjunto com o Ministério do Planejamento, Orçamento e Gestão, proposta de regularização da situação jurídica dos seus recursos humanos, que deverá conter, necessariamente:*

a) o quantitativo de pessoal necessário para substituir trabalhadores terceirizados que estejam em desacordo com o Decreto n° 2.271, de 7 de junho de 1997;

b) o quantitativo de cargos, empregos e/ou funções públicas a serem criados, se for o caso;

c) a previsão de realização de concursos públicos para a admissão de novos servidores e/ou empregados públicos;

d) o impacto orçamentário-financeiro das medidas;

e) o cronograma de execução.

***Parágrafo 2°** O ato que autorizar a realização de concurso público deverá prever expressamente que os novos provimentos estarão vinculados ao pleno cumprimento das obrigações assumidas no presente Termo de Conciliação.*

***Parágrafo 3°** O Ministério do Planejamento, Orçamento e Gestão deverá adotar todas as medidas necessárias no âmbito de sua competência para a regularização da situação jurídica dos recursos humanos de cada órgão da Administração Pública Federal, como autorização para a realização de concursos públicos, encaminhamento de projetos de lei relativos à reestruturação de carreiras e à criação de novos cargos, empregos e/ou funções públicas e previsão de disponibilidade orçamentaria para cobrir as novas despesas.*

***CLÁUSULA TERCEIRA.** O adimplemento das obrigações ora ajustadas obedecerá rigorosamente ao cronograma a seguir estabelecido:*

*a) até **31/07/2008,** deverão estar concluídas, pelo Ministério do Planejamento, Orçamento e Gestão, as propostas de regularização da situação jurídica dos recursos humanos de todos os órgãos da administração pública federal, com fundamento em estudos que demonstrem as reais necessidades da força de trabalho realizada pêlos terceirizados*

*b) até **31/07/2009,** a União deverá substituir, no mínimo, 30% do pessoal terceirizado que esteja realizando atividades incompatíveis com o presente Termo de Conciliação por trabalhadores admitidos mediante concurso público, nos termos do art. 37, II, da Constituição Federal;*

*c) até **31/12/09,** a União deverá substituir, no mínimo, mais 30% do pessoal terceirizado que esteja realizando atividades incompatíveis com o presente Termo de Conciliação por trabalhadores admitidos mediante concurso público, nos termos do art. 37, II, da Constituição Federal;*

*d) até **31/12/10,** a União deverá substituir todo o pessoal terceirizado que esteja realizando atividades incompatíveis com o presente Termo de Conciliação por trabalhadores admitidos mediante concurso público, nos termos do art. 37, II, da Constituição Federal, ultimando a adequação de que trata a cláusula segunda do presente Termo de Conciliação.*

***Parágrafo Único** - Compete ao Ministério do Planejamento, Orçamento e Gestão.autorizar a realização dos respectivos concursos públicos, obedecidos os devidos preceitos legais.*

***CLÁUSULA QUARTA.** A União se compromete a recomendar o estabelecimento das mesmas diretrizes ora pactuadas em relação às autarquias, fundações públicas, empresas públicas e sociedades de economia mista, a fim de vincular todos os órgãos integrantes da administração pública indireta ao cumprimento do presente termo de conciliação, sendo que em relação às empresas públicas e sociedades de economia mista deverá ser dado conhecimento ao Departamento de Coordenação e Controle das Empresas Estatais - DEST, do Ministério do Planejamento, Orçamento e Gestão.*

***CLAUSULA QUINTA.** O descumprimento das obrigações assumidas no presente Termo de Conciliação sujeitará a União à multa (astreinte) correspondente a R$ 1.000,00 (um mil Reais), por obrigação descumprida (cláusulas e/ou seus parágrafos, incisos ou alíneas), por trabalhador encontrado em situação jurídica irregular, reversível ao Fundo de Amparo ao Trabalhador - FAT, nos termos dos arts. 5°, § 6°, e 13 da Lei n° 7.347, 24 de julho de 1985, com obrigatório regresso em desfavor do agente público responsável, independentemente das demais cominações e providências que poderão vir a ser requeridas pelo Ministério Público do Trabalho.*

Parágrafo 1° A cobrança da multa não desobriga a UNIÃO do cumprimento das obrigações contidas no presente Termo de Conciliação.

Parágrafo 2° Independentemente das autoridades indicadas como diretamente responsáveis pelo cumprimento do presente Termo de Conciliação, o agente público que, em nome da Administração Pública Federal, firmar ou permitir que terceiros

estranhos à Administração, firmem contrato de prestação de serviços em contrariedade às disposições estabelecidas no presente Termo de Conciliação, será responsável solidário por qualquer contratação irregular, respondendo pela multa prevista no caput desta cláusula, além de outras sanções administrativas e penais cabíveis.

***CLÁUSULA SEXTA**. O presente Termo de Conciliação produzirá efeitos legais a partir da sua celebração, devendo ser submetido ao MM. Juízo da 17a Vara do Trabalho de Brasília/DF para homologação, a fim de conferir-lhe eficácia de título executivo judicial.*

Estando assim, justos e compromissados, firmam o presente instrumento, para que produza os seus efeitos legais.

Brasília, 05 de novembro de 2007.

José Antonio Dias Toffoli
Advogado-Geral da União

Paulo Bernardo Silva
Ministro de Estado do Planejamento, Orçamento e Gestão

Otávio Brito Lopes
Procurador-Geral do Trabalho

Luís Henrique Martins dos Anjos
Procurador-Geral da União

Fábio Leal Cardoso
Procurador do Trabalho

Vivian Rodrigues Mattos
Procuradora do Trabalho