doi: 10.5102/un.gti.v2i1. 1681

Fatores culturais e estruturais que impactam na implantação da política de segurança da informação: um estudo de caso sobre o ministério do desenvolvimento agrário*

Cultural and structural factors that impact on the implementation of information security policy: *a case study of the ministry of agrarian development*

Eduardo Camargos L. do Nascimento[1]

Resumo

Os fatores culturais e estruturais estão entre os que mais implicam na adoção de fato de uma política em segurança da informação no âmbito dos ministérios, o que tem se mostrado um grande desafio para as áreas gestoras dessa esfera. Ao considerar aspectos culturais, legais, estruturais, políticos e de recursos humanos, pode-se identificar o quão complexo é implantar qualquer tipo de campanha, política ou governança. O governo brasileiro vive um momento de necessidade de mudanças e modernização no pensamento organizacional em que as boas práticas de governança e segurança da informação deixam de ter um caráter meramente sugestivo e passam a ser exigência, até mesmo dentro de uma perspectiva legal. Isto requer uma análise mais profunda de seus métodos de trabalho e estruturas organizacionais e que, uma vez revistos, pode envolver uma profunda mudança de cultura e conformidade com normas e procedimentos pouco comuns outrora e de complexa implantação e consolidação.

Palavras-chave: Segurança da informação. Cultura organizacional. Governança em tecnologia da informação.

Abstract

The structural and cultural factors are among the most critical aspects in the adoption of a full policy of security information in the organizations, which has proved a challenge for the management areas of this sphere. When considering the cultural, legal, structural, political and human resources, becomes complex to deploy any kind of change or policy aimed to information security. The Brazilian government is experiencing a moment of need for change and modernization in organizational thinking in which good governance practices and information security no longer have a merely suggestive concept and are now a real demand, even within a legal perspective. This requires a deeper analysis of its working methods and organizational structures and, if revised, may involve a profound change of culture for the compliance with norms and procedures not so common in the past and with complex implementation and consolidation

Keywords: Information security. Organizational culture. IT Governance.

* Artigo recebido em 19/11/2011
Aprovado em 23/04/2012

[1] Graduado em Segurança da Informação, com Especialização em Governança de Tecnologia da Informação e em Redes e Telecomunicações. É certificado *ITIL V3 Foundations* e BPM Fundamentals. Atualmente, é coordenador de infraestrutura de TI no Ministério do Desenvolvimento Agrário.

1 Introdução

A Tecnologia das Informações e os Sistemas Organizacionais tornaram-se um dos principais fatores de sucesso para as organizações. As informações são um bem não palpável, mas que influenciam diretamente em todos os negócios de uma empresa ou de um indivíduo. E no âmbito governamental, envolve desde os programas de governo, informações intrínsecas à estrutura dos órgãos, os seus projetos e até dados utilizados por órgãos de controle e fiscalização.

Muitas organizações sofrem ameaças constantes em seus ativos, o que, em caso de incidentes, representa um prejuízo incalculável. A gama de vulnerabilidades em ambientes corporativos voltados à Tecnologia da Informação, ultrapassa barreiras tecnológicas, pois começa a surgir um cenário em que a cultura organizacional, processos, governança e cultura são fatores essenciais para que se garanta uma relativa segurança e logo, a disponibilidade das informações.

O que aconteceria se ocorresse a perda dos dados importantes de uma organização governamental devido a uma enchente, a um incêndio ou a uma violação de segurança? Pode-se exemplificar o fatídico incêndio do prédio do Ministério da Previdência Social em 2005, em Brasília. Será que a organização estava pronta para tratar esse tipo de incidente? Quanto tempo levaria para que ela recuperasse todos os dados perdidos? A maioria das organizações governamentais não tem capacidade de se recuperar desses tipos de incidentes, apesar de muitas vezes terem instituídas e aprovadas pelos mais altos escalões, uma política de segurança da informação.

Isso ocorre, dentre outros motivos, porque, apesar da força de lei que as obriga a terem uma política de segurança da informação que contemple a disponibilidade, a confidencialidade, a integridade, a recuperação, o contingenciamento e a gestão dos ativos de informação, nem sempre é dada a devida importância e tampouco essa política é bem aceita, seguida ou mesmo compreendida pelos diversos setores da organização. É esse cenário um dos grandes desafios de órgãos do Governo Federal brasileiro.

Este artigo pretende identificar os motivos desse desafio em uma perspectiva cultural e estrutural, se existe a subordinação a uma série de forças legais que exigem que se tenha e que se cumpram procedimentos de segurança das informações e por que é tão penoso colocar em prática essas ações. Quais desenhos estruturais e burocráticos impedem que ela seja implantada? Que legislações podem alavancar a implantação destes processos e qual a perspectiva dos usuários finais, gestões e líderes de governo tem quanto a esse tipo de iniciativa? Neste artigo, objetivou-se realizar uma análise de alguns desses fatores e avaliar qual o seu impacto na implantação da política de segurança da informação e, para que isso seja possível, serão buscadas respostas analisando aspectos culturais, estruturais, legais, o ambiente de tecnologia da informação e, por que não, aspectos humanos, utilizando como objeto de pesquisa o Ministério do Desenvolvimento Agrário, pela facilidade do autor ao ambiente e aos dados expostos.

Uma política de segurança da informação assegura, dentre muitos fatores justificados por sua grande abrangência, que as informações estejam sempre disponíveis, íntegras e confiáveis. Em um contexto governamental, isso significa o controle sobre projetos, sobre gastos públicos, sobre políticas de governo e, principalmente, pela prestação de um serviço melhor à sociedade. Esta pesquisa se justifica uma vez que é evidente a necessidade de um aprofundamento na visão do papel da segurança da informação nas estruturas governamentais, visando identificar se são efetivas e eficazes de fato, e se não o forem, quais os fatores que impedem que sejam. A segurança da informação no segmento privado é uma realidade há mais de uma década e pode-se perceber um atraso das estruturas do governo em relação a isso, e partindo do pressuposto de valor das informações, sabe-se que envolvem interesses de segurança nacional e desenvolvimento do país.

Para o autor, esta pesquisa é importante pois, além de compor o quadro de servidores não efetivos de um órgão do Governo Federal, atua na área de Tecnologia da Informação e, indiretamente, na área de segurança da informação e vislumbra a necessidade de debates mais profundos sobre o tema.

Dessa forma, faz-se necessário o seguinte questionamento: Quais os fatores culturais e de estrutura do Governo, especificamente do Ministério do Desenvolvimento Agrário, que impactam na implantação efetiva de uma Política de Segurança das Informações?

O método de pesquisa utilizado, quanto aos fins, será descritivo na medida em que estabelece relação entre as variáveis estudadas, descrevendo as características ou fenômenos da população estudada (VERGARA, 2007); e,

quanto aos meios, será utilizado o método de pesquisa bibliográfica e de campo. Sobre a pesquisa bibliográfica, Cervo e Bervian (2002, p. 65) acrescentam ainda: "A pesquisa bibliográfica procura explicar um problema a partir de referências teóricas publicadas em documentos. Pode ser realizada independentemente ou como parte da pesquisa descritiva ou experimental".

Sobre a pesquisa de campo, observa-se que tem por objetivo, de forma prioritária, a busca de dados e/ou conhecimentos sobre um problema, sobre o fenômeno espontâneo, por acontecer no próprio local onde correm os fenômenos ou onde está a população estudada (MARKONI; LAKATOS, 2008).

Foram coletados dados por meio de um questionário fechado, aplicado no Ministério do Desenvolvimento Agrário para servidores efetivos, comissionados e terceirizados de todos os níveis, ou seja, tático, estratégico e operacional. Esse método foi escolhido uma vez que torna a resposta impessoal e por ser de fácil aplicação, além de representar uma percepção genuína da opinião dos colaboradores sobre as questões abordadas pela pesquisa. Para melhor aceitação do questionário, ele foi disponibilizado por meio de formulário em uma página na *intranet* do Ministério.

Este artigo estrutura-se em dois tópicos: O desenvolvimento e análises e considerações finais. No primeiro, há uma explanação sobre a estrutura do Governo Federal, sobretudo a estrutura do Ministério do Desenvolvimento Agrário, suas atribuições, planos de governo e princípios para que os valores da organização sejam mensurados. Ainda, é exposta a gama de autores que escreveram sobre temas pertinentes a este artigo, formando o referencial teórico, dividido em subcapítulos por temas macros, tais como segurança da informação, cultura organizacional e conformidade com legislações e boas práticas voltadas à Segurança da Informação, e algum conteúdo sobre Governança em Tecnologia da Informação, uma vez que é praticamente impossível ter aspectos de segurança e cultura organizacional interligados sem que estejam atrelados a princípios consistentes de governança. Na última parte - análises e considerações finais - consta a consolidação dos dados coletados com todas as considerações, análises pertinentes e os resultados da pesquisa. Por último, estão os anexos I e II, e posteriormente, as referências bibliográficas utilizadas no decorrer da elaboração do artigo.

2 Desenvolvimento

2.1 Um olhar sobre os ministérios

Os ministérios são órgãos do Poder Executivo, da administração direta, e atualmente no Brasil existem 31 ministérios e órgãos essenciais e cinco secretarias especiais com status de ministério. Cada ministério representa uma área, ou seja, é um departamento do governo, liderado por um ministro que é indicado pelo Presidente da República no período de cada mandato. De acordo com o "Portal Brasil" (Brasil.gov.br) "Os ministérios criam normas, acompanham e avaliam programas federais e implantam políticas para os setores que representam". Logo, esses órgãos trabalham na gestão e aplicação de recursos, planos e estratégias de governo para áreas específicas. Em áreas estratégicas, como a segurança institucional e os direitos humanos, o Governo possui secretarias, e o secretário de cada uma tem *status* de ministro.

Estruturalmente, os ministérios são divididos em gabinete, secretarias, subsecretarias, coordenações, assessorias e até diretorias que variam de acordo com o órgão. Fundamental e estruturalmente, os ministérios podem ser vistos da seguinte forma:

Figura 1: Organograma típico

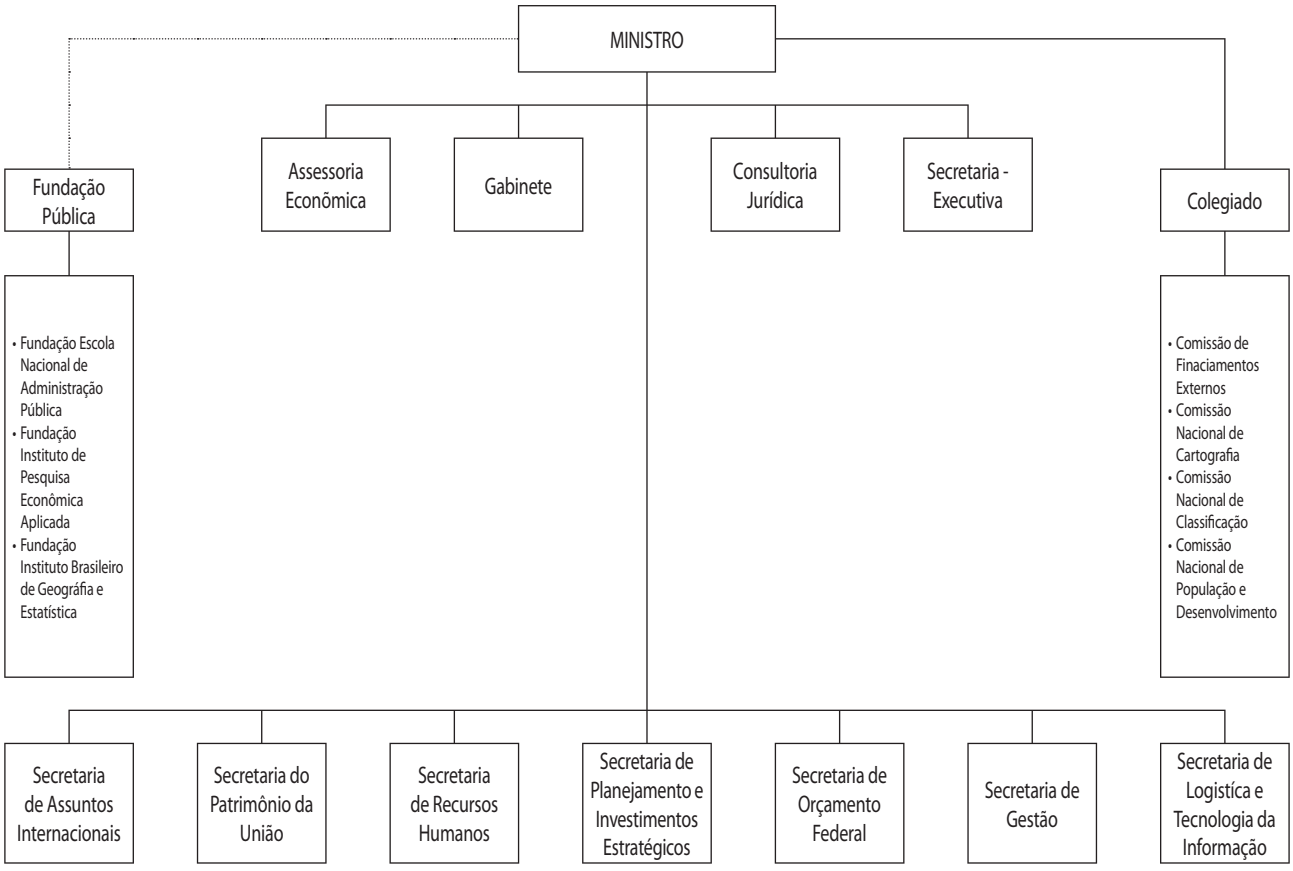
Fonte: Desenvolvido pelo autor em 2011.

Esta é uma estrutura básica, porém, na maioria das vezes, há muito mais vinculações com assessorias e secretarias ligadas diretamente ou não ao gabinete e com características relacionadas à natureza do ministério. Um exemplo de organograma ministerial diferenciado é o do Ministério do Planejamento, Orçamento e Gestão, conforme mostra a Figura 2. Além da Assessoria Jurídica, da Secretaria Executiva e do Gabinete, existe ainda uma Assessoria Econômica diretamente subordinada ao ministro. Existem também diversas outras secretarias subordinadas ao ministro e um Colegiado e uma Fundação Pública diretamente vinculados, e não subordinados, caracterizados na imagem por linhas pontilhadas.

Abaixo das secretarias, geralmente estão os departamentos e setores voltados à atividade-fim do órgão. E por mais que não seja uma regra, na grande parte dos

ministérios, abaixo da Secretaria Executiva, que tem por atribuição, dentre outras, assistir ao Ministro de Estado na supervisão e coordenação das atividades das secretarias integrantes da estrutura do ministério e das entidades a ele vinculadas, está a Subsecretaria de Planejamento, Orçamento e Administração (SPOA). As SPOA's são supervisionadas pelas secretarias executivas e têm em seu fundamento planejar, coordenar e supervisionar a execução das atividades relacionadas com os sistemas federais de organização e modernização administrativa, de recursos humanos, de serviços gerais, de administração dos recursos de informação e informática, de planejamento e de orçamento, de contabilidade e de administração financeira, no âmbito do ministério ao qual está vinculada; portanto, os diversos setores de cunho administrativo, financeiro, de serviços gerais e de tecnologia da informação, salvo algumas exceções.

Figura 2: Organograma diferenciado.



Fonte: Disponível em: <http://www.dicasdebrasilia.com.br/005>. Acesso em: 01 maio 2011.

2.2 O ministério do desenvolvimento agrário

O Ministério do Desenvolvimento Agrário teve sua estrutura regimental regulamentada conforme Decreto nº 7.255 de 4 de agosto de 2010, com vigência a partir de 1° de setembro de 2010, conforme Decreto n° 7.280, de 31 de agosto de 2010.

O órgão tem por competência as seguintes atribuições:

I - reforma agrária;

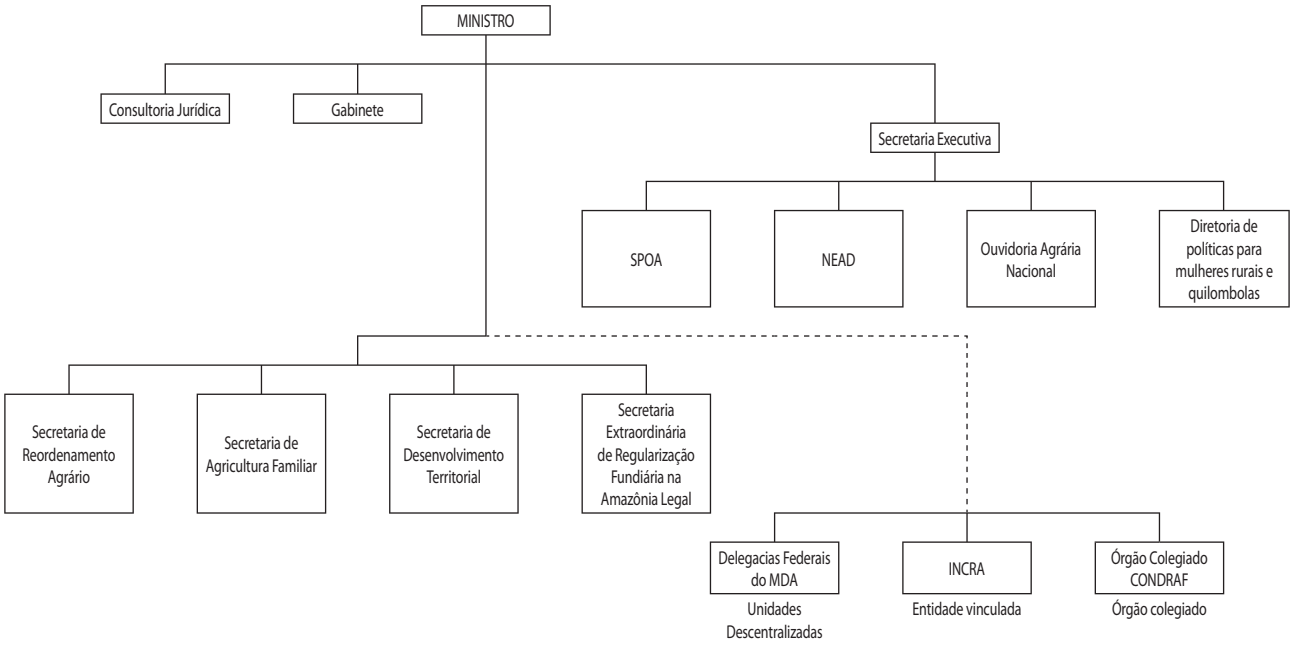
II - promoção do desenvolvimento sustentável do segmento rural constituído pelos agricultores familiares; e

III - identificação, reconhecimento, delimitação, demarcação e titulação das terras ocupadas pelos remanescentes das comunidades dos quilombos.

Parágrafo único. O Ministério do Desenvolvimento Agrário exercerá, em caráter extraordinário, as competências relativas à regularização fundiária na Amazônia Legal de que trata o art. 33 da Lei no 11.952, de 25 de junho de 2009 (BRASIL, Decreto nº 7.255, de 4 de agosto de 2010).

Abaixo o organograma do Ministério do Desenvolvimento Agrário:

Figura 3: Organograma do MDA



Fonte: Desenvolvido pelo autor em 2011.

Como de praxe, a estrutura segue o modelo clássico da maioria dos ministérios com Gabinete, Consultoria Jurídica e Secretaria Executiva subordinados diretamente ao ministro. Posteriormente, as secretarias, referenciadas pelo Decreto como "[...] órgãos específicos singulares" e por último as unidades descentralizadas, que são as Delegacias Federais do MDA, o órgão colegiado ou Conselho Nacional de Desenvolvimento Rural Sustentável (CONDRAF) e o Instituto Nacional de Colonização e Reforma Agrária (INCRA), como entidade vinculada.

Esse organograma foi criado a partir do Decreto que instituiu o Ministério do Desenvolvimento Agrário, porém, posteriormente, houve algumas alterações, principalmente no âmbito do Gabinete, cujo portal do MDA define como "[...] é formado pela Assessoria, Assessoria de Comunicação Social, Assessoria Internacional de Promoção Comercial e Assessoria Parlamentar e Coordenação-Geral Nacional das Delegacias Federais do Desenvolvimento Agrário". Todavia, este artigo considerará a estrutura fundamental do órgão para realizar suas análises, uma vez que a criação de setores e departamentos muda dinamicamente com as idas e vindas de governos e a partir de diretrizes políticas.

O Ministério do Desenvolvimento Agrário é relativamente novo e pode ser considerado um órgão pequeno, com cerca de 1000 (mil) colaboradores entre servidores estáveis e comissionados, terceirizados, consultores do Programa das Nações Unidas para o Desenvolvimento (PNUD) e estagiários. A maior parte de sua estrutura está no Palácio do Desenvolvimento, no centro de Brasília; porém, há alguns setores ligados diretamente ao Gabinete como a Consultoria Jurídica e a Assessoria Internacional de Promoção Comercial, por exemplo, que estão com o Gabinete na Esplanada dos Ministérios. Fora as localidades citadas, há ainda setores espalhados por pelo menos dois prédios na capital.

A título de contextualização, é importante abordar as atividades relacionadas às Secretarias do MDA, a saber:

Secretaria da Agricultura Familiar (SAF):

A Secretaria da Agricultura Familiar (SAF) tem por missão consolidar o conjunto da agricultura familiar de modo a promover o desenvolvimento local sustentável.

Secretaria de Reordenamento Agrário (SRA):

A Secretaria de Reordenamento Agrário (SRA) atua na implementação de políticas públicas nacionais para o meio rural por meio de ações complementares à Reforma Agrária, como a garantia de acesso a terra pelo Crédito Fundiário.

Secretaria de Desenvolvimento Territorial (SDT):

A Secretaria de Desenvolvimento Territorial (SDT) contribui para o desenvolvimento harmônico de regiões onde predominam agricultores familiares e beneficiários da reforma e do reordenamento agrários.

A Secretaria Executiva, além de todo apoio ao Gabinete na coordenação, supervisão e acompanhamento de programas e projetos ligados às estratégias do órgão, é a área diretamente ligada à Subsecretaria de Planejamento, Orçamento e Administração (SPOA). Para fins deste artigo, o setor será analisado com mais atenção, pois é nele que se encontra o núcleo da área de Tecnologia da Informação do órgão, que dará base para o alcance dos objetivos de pesquisa.

A SPOA tem por competência:

I - planejar e coordenar a execução das atividades de organização e modernização administrativa, bem como as relacionadas com os sistemas federais de recursos humanos, de serviços gerais, planejamento e orçamento, de administração financeira, de contabilidade e de recursos da informação e informática, no âmbito do Ministério (BRASIL. Art. 50 da Lei nº 10.683, de 28 de maio de 2003).

Em sua composição, a SPOA tem as seguintes coordenações:

Coordenação Geral de Modernização e Informática – CGMI

Coordenação Geral de Administração e Recursos Humanos – CGARH

Coordenação Geral de Planejamento e Orçamento – CGPO

Coordenação Geral de Finanças, Convênios e Contabilidade – CGFCC

Embora, haja uma Coordenação Geral de Modernização e Informática, cada uma das secretarias citadas possui uma área independente de Tecnologia da Informação com desenvolvimento de sistemas e áreas de negócios de sistemas quase totalmente autônomas e que apenas utilizam a estrutura do Ministério para o desenvolvimento de suas atividades, muitas vezes sem passar pelo crivo da CGMI.

O MDA, em sua estrutura, abriga sistemas que dão apoio às suas estratégias de negócio e, apesar de ser um órgão relativamente pequeno, seus projetos e programas de governo têm alcançado grandes dimensões, principalmente quando o atual governo declarou que a agricultura familiar é prioridade e realizou ações de incentivo a ela como a redução de juros e liberação de cerca de 16 bilhões de reais para os pequenos agricultores do país, como pode ser visto no sítio: <http://blog.planalto.gov.br/assunto/agricultura-familiar/>.

Programas de governo como o Programa Nacional de Fortalecimento da Agricultura Familiar (PRONAF), que financia projetos individuais ou coletivos que gerem renda aos agricultores familiares e assentados da Reforma Agrária e o Programa de Regularização Fundiária, que deve entregar títulos de terras a cerca de 300 mil posseiros que ocupam terras públicas federais não destinadas, ou seja, que não sejam reservas indígenas, florestas públicas, unidades de conservação, áreas de fronteira, marinha ou reservadas à administração militar, são programas de alto valor para a sociedade e trabalham com informações confidenciais e estratégicas até para a segurança nacional, quando se fala em liberação de crédito e proteção da Amazônia.

Esses e muitos outros sistemas estão indiretamente ou diretamente ligados à CGMI e sua infraestrutura de redes, comunicações, internet, maquinário de tecnologia abarca toda a inteligência e estratégia do Ministério.

2.3 Cultura organizacional

Sabe-se que as instituições, desde sua concepção, começam a formar o que os teóricos chamam de cultura organizacional. A cultura é um fator de grande importância dentro das organizações, pois é ela que permite a adoção bem sucedida de novas diretrizes da empresa, mudanças de rumo, mudança na abordagem estratégica, implantação de normas e procedimentos e impacta diretamente em aspectos motivacionais dos colaboradores. Uma cultura traz traços identitários da organização e revela a percepção de valores dos funcionários e, principalmente, a forma como a alta gestão conduz as mais diversas situações, tanto em momentos positivos quanto em momentos críticos. De acordo com Certo (2003, p. 384), a cultura organizacional é "[...] um conjunto de valores e crenças partilhados que os colaboradores têm a respeito do funcionamento e da existência da organização". Existem várias correntes de pensadores sobre o tema da cultura organizacional, que passou a ser discutida a partir da década de 1980 com a publicação de artigos em periódicos específicos das cadeiras de Administração como o *Administrative Science Quaterly, Organization Studies,* dentre outros (AKTOUF, 1994, p. 40).

A cultura vigente de uma organização pode servir como termômetro em termos motivacionais e pode

levar a um comprometimento total dos funcionários ou a rendimentos que beiram o medíocre em caso de falta de comprometimento e de entendimento e concordância com os objetivos da organização.

O desenvolvimento de uma cultura, segundo algumas linhas teóricas, pode ser moldado e dinâmico, consonante com os objetivos, os valores e a visão da organização e de seus criadores e gestores, e resultante de uma série de fatores externos, como os da sociedade na qual a organização está inserida. Sobre isso, Chiavenato (2005, p. 225) afirma que a cultura de uma organização "[...] é um conjunto de hábitos e crenças, estabelecidos através de normas, valores, atitudes e expectativas compartilhadas por todos os membros da organização". Essa visão é interessante, pois pode revelar em uma mesma sociedade nuances diferenciadas de culturas organizacionais, uma vez que se realize uma análise de diversos setores da sociedade: Quais fatores externos e sociais influenciam na cultura da uma empresa da iniciativa privada que tem que cumprir metas, garantir o lucro e a expansão em função de sobrevivência e permanência no mercado? Ou, no terceiro setor, em que o lucro não é visado, como é trabalhada a questão dos objetivos organizacionais? Da mesma forma, na esfera pública podem existir fatores definitivos para o desenvolvimento e mutação de uma cultura e, talvez, aspectos cruciais para que isso ocorra sejam as particularidades legais que regem o funcionalismo público unido a uma herança arcaica de comportamento e culturas de governo e por fim, o aspecto político partidário.

Nesse universo de discussões sobre a cultura organizacional, há divergência na linha de pensamento dos autores sobre o tema. Existe uma corrente voltada para uma análise antropológica da cultura organizacional assim como, uma análise com o viés mais acadêmico voltado à administração. O artigo "Cultura organizacional em organização pública: as bases da mudança organizacional a partir da reforma gerencial", traz uma abordagem detalhada sobre o tema e remete ao seguinte questionamento: Se a cultura para alguns autores se constitui de elementos materiais e imateriais, símbolos e mitos que são criados a partir da história de cada povo, como seria possível aos dirigentes e estudiosos da cultura organizacional pensar em transformação dessa mesma cultura? E, além disso, como entende Hofstede que a cultura organizacional sofre influência da nacionalidade em que se encontra a organização, seria possível transformar uma cultura organizacional a partir da vontade de seus dirigentes? (SILVA; FADUL, 2006).

Na perspectiva de Certo (2003), sete características básicas e unidas captam a essência da cultura de uma organização. São elas: inovação e ousadia, ou seja, a capacidade e o incentivo de inovar e correr riscos dos colaboradores da organização; atenção ao detalhe, que contempla a atenção ao nível de análise e atenção aos detalhes; busca por resultados, o quão a organização está empenhada em alcançar resultados em vez de apenas como ela vai alcançar esses resultados, como por exemplo, pelos processos e procedimentos dos quais ela faz uso; concentração nas pessoas, o nível de valor humano para a corporação, e o grau de consideração que a alta gestão tem ao tomar decisões que influenciam nas pessoas; orientação para equipe, o que é pensado mais em prol das equipes do que em prol de indivíduos isolados; agressividade, o grau em que as pessoas são mais agressivas e competitivas e, por último, a estabilidade, o quão a organização se mantém estável mesmo em processo de constante crescimento.

Porém, essas características básicas citadas por Certo (2003), possuem características mais compatíveis com empresas da iniciativa privada, que geralmente possuem uma cultura forte, em que os valores da organização são altamente assumidos, compreendidos e compartilhados. Em organizações assim, pode-se perceber o conhecimento dos valores pela percepção do mais baixo cargo ao mais alto escalão. Essa análise não pode ser aplicada totalmente a organizações governamentais. Mesmo a cultura sendo formada por valores nacionais e sociais, as características de empresas do governo diferem, e muito, de empresas da iniciativa privada.

Aspectos históricos e da própria formação do Brasil como nação revelam traços de como foi conduzida e formada a cultura de organizações do Estado. A herança lusitana, os diversos períodos do governo como, o getulismo, as ditaduras, a democracia, a Lei nº 8.112/90, que instituiu o regime jurídico dos servidores públicos civis da União, Autarquias, inclusive as especiais, e as Fundações Públicas Federais, contribuíram diretamente para o que é a cultura organizacional do governo brasileiro. (MOTTA; CALDAS, 1997).

Em seu artigo "Cultura Organizacional em Organizações Públicas no Brasil", Pires e Macedo (2006, apud GUIMARÃES, 2000, p.127) afirmam:

> [...] no setor público, o desafio que se coloca para a nova administração pública é como transformar estruturas burocráticas, hierarquizadas e que tendem a um processo de insulamento em organizações flexíveis e empreendedoras.

Assim, se a cultura organizacional é fundamentada em aspectos estruturais da organização, como o direcionamento da alta gestão, e por fatores externos como a nacionalidade e os diversos fatores da sociedade, a cultura dos órgãos do governo são diretamente afetadas por variáveis, uma vez que se faz a seguinte análise:

O tempo de mandato: passado o tempo de mandato, é de praxe que o corpo não funcional do órgão seja profundamente alterado, principalmente em se tratando da parte estratégica. Isso implica também em uma provável, e quase certa, mudança de direcionamento, seja por ideologia, interesses ou diretrizes do novo governo.

Órgãos do governo, em sua maioria, não buscam lucro; sua responsabilidade é com a sociedade e nem sempre os objetivos estratégicos estão claros para os funcionários, tanto do corpo efetivo quanto dos demais.

Em empresas da iniciativa privada, principalmente as de cultura forte, se o funcionário não estiver de acordo com as metas da corporação, geralmente ele se desliga ou é desligado. No governo, existe a estabilidade que mantém o funcionário independente de corresponder aos objetivos estratégicos do órgão.

Existe uma dependência de recursos e aprovações de órgãos externos. Uma vez que os centros de poder são distribuídos entre diversos partidos, não há efetividade de alcance de um objetivo caso não haja interesses compatíveis.

Esses fatores caracterizam as empresas do governo e refletem a distância que as separa da cultura que é mais comum às corporações privadas. Conforme Carbone (2000, p. 234), essas são algumas características de organizações públicas do Brasil:

burocratismo — excessivo controle de procedimentos, gerando uma administração engessada, complicada e desfocada das necessidades do país e do contribuinte;

autoritarismo/centralização — excessiva verticalização da estrutura hierárquica e centralização do processo decisório;

aversão aos empreendedores — ausência de comportamento empreendedor para modificar e se opor ao modelo de produção vigente;

paternalismo — alto controle da movimentação de pessoal e da distribuição de empregos, cargos e comissões, dentro da lógica dos interesses políticos dominantes;

levar vantagem — constante promoção da punição àqueles indivíduos injustos, obtendo vantagens dos negócios do Estado; e

reformismo — desconsideração dos avanços conquistados, descontinuidade administrativa, perda de tecnologia e desconfiança generalizada. Corporativismo como obstáculo à mudança e mecanismo de proteção à tecnocracia (grifos nossos).

2.4 A segurança da informação

A competitividade e o dinamismo do mundo contemporâneo fazem com que as empresas e os governos invistam cada vez mais em sistemas de informação interligados, com vista a aprimorar os processos internos, cortar custos e ter maior competitividade. Porém, na proporção em que cresce a dependência por esses sistemas, também cresce a gama de riscos aos quais essas organizações estão submetidas. Dados sigilosos de governos ou segredos industriais devem ser protegidos e podem culminar no sucesso ou no fracasso de um projeto. Nesse cenário, surge a segurança da informação, que possui muitas nuances, desde uma perspectiva de negócio à camada mais baixa de um sistema operacional.

Conforme Dias (2000**,** p. 41), a segurança das informações é, "[...] portanto, a proteção de informações, sistemas, recursos, e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança".

O Guia para Gestão de Segurança da Informação do Instituto IT Governance conceitua segurança da informação da seguinte forma:

A Segurança da Informação envolve um universo de riscos, benefícios e processos envolvidos com todos os recursos de informações disponíveis. Tornou-se claro que as informações devam ser tratadas com o mesmo cuidado e prudência que os outros ativos organizacionais.

A segurança da informação deve preservar a permanência de alguns fundamentos essenciais, tais como confidencialidade, integridade e disponibilidade. Sobre isso, Moreira (2001, p. 9) diz que "[...] o objetivo da segurança, no que tange à informação, é a busca da disponibi-

lidade, confidencialidade e integridade dos seus recursos e da própria informação".

Esses são conceitos primordiais, porém, alguns autores ainda falam sobre não repúdio, autenticidade, consistência e auditoria, dentre outros. Dias (2000, p. 42) conceitua esses fundamentos como:

Confidencialidade – proteger as informações contra o acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação, isto é, as informações e processos são liberados apenas a pessoas autorizadas [...]; **integridade** – evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação [...]. O conceito de integridade está relacionado com o fato de assegurar que os dados não foram modificados por pessoas não autorizadas [...]; **disponibilidade** – proteger os serviços de informática de tal forma que não sejam degradados ou tornados indisponíveis quando se necessita dele [...]. Disponibilidade pode ser definida como a garantia de que os serviços prestados por um sistema são acessíveis, sob demanda, aos usuários ou processos autorizados (grifos nossos).

O não repúdio e a autenticidade são conhecidos como a responsabilidade final, que tem como objetivo verificar a identidade e autenticidade da fonte da informação, interna ou externa, garantindo a integridade de origem da informação (PEIXOTO, 2006).

Em outra abordagem, a autenticidade é a necessidade de verificar que uma comunicação, transação ou acesso a algum serviço é legitimo enquanto o não repúdio seria a impossibilidade de um remetente negar que enviou determinada mensagem (ALVES, 2006).

De acordo com Dias (2000, p. 42) a consistência "[...] certifica-se de que o sistema atua de acordo com as expectativas dos usuários autorizados [...]", e a auditoria visa "[...] proteger os sistemas contra erros e atos maliciosos cometidos por usuários autorizados". Isto é, enquanto um garante o funcionamento esperado pelo pessoal autorizado de uma solução, o outro garante que esse pessoal não corrompa, adultere ou modifique essa solução com objetivos maliciosos.

Para Silva, Carvalho e Torres (2003, p. 17):

> A preservação da confidencialidade, integridade e disponibilidade da informação utilizada nos sistemas de informação requer medidas de segurança, que por vezes também são utilizadas como forma de garantir a autenticidade e o não repúdio.

Como se pode perceber, muitos desses conceitos estão inter-relacionados, mas para fins deste artigo, utilizar-se-ão apenas os pilares confidencialidade, integridade e disponibilidade.

Esses conceitos justificam-se uma vez que são aplicados para proteger os principais bens das organizações, que são seus ativos. Ativos são as informações importantes de seu sistema, aquilo que pode ser destruição (ALBUQUERQUE; RIBEIRO, 2002). De forma mais abrangente, Moreira (2001, p. 20) descreve ativo como "[...] tudo que manipula direta ou indiretamente uma informação, inclusive a própria informação [...], e é isso que deve ser protegido contra ameaças para que o negócio funcione corretamente".

Os ativos de uma organização ainda podem ser o meio em que a informação trafega, em que é armazenada, os equipamentos em que ela é manuseada e descartada (SÊMOLA, 2006).

O ativo de uma empresa, portanto, é qualquer informação de valor, muitas vezes não é tangível, mas tem uma importância vital para a manutenção e continuidade do negócio e que necessita de proteção. Ferreira (2003, p. 23-24, grifo nosso) classifica as informações em 4 classes:

> **Classe 1**: Pública/informação não classificada: Informações que, se forem divulgadas fora da organização, não trarão impactos aos negócios. A integridade dos dados não é vital. **Classe 2**: Informação interna: O acesso externo às informações deve ser evitado. Entretanto, se estes dados tornarem-se públicos, as conseqüências não são críticas. A integridade dos dados é importante, mas não vital. **Classe 3**: Informação confidencial: As informações desta classe devem ser confidenciais dentro da organização e protegidas de acesso externo. Se alguns destes dados forem acessados por pessoas não autorizadas, as operações da organização podem ser comprometidas, causando perdas financeiras e perda de competitividade. A integridade dos dados é vital. **Classe 4**: Informação secreta: O acesso interno ou externo não autorizado a estas informações é extremamente crítico para a organização. A integridade dos dados é vital. O número de pessoas com acesso as informações deve ser muito pequeno, bem como regras restritas para sua utilização.

Como ocorrem os ataques aos ativos das organizações? Na maioria das vezes, o ataque, que ocasiona indisponibilidade, furto ou corrompimento de informações,

é proveniente da exploração de uma vulnerabilidade na sistemática da organização que abrange pessoas, processos, instalações físicas, políticas internas e, claro, computadores e sistemas.

A vulnerabilidade é o ponto em que qualquer sistema está suscetível a um ataque. Trata-se de uma condição causada muitas vezes pela ausência ou falta de efetividade das medidas que visam salvaguardar os bens da organização (MOREIRA, 2001).

O incidente causado pela exploração de uma vulnerabilidade é a concretização de uma ameaça. Para Sêmola (2006, p. 46), as ameaças "[...] são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de uma vulnerabilidade".

A combinação desses elementos, vulnerabilidade e ameaça, somada ao dano ou impacto que eles causariam ao ativo, é chamado de risco. Para Dias (2000, p. 54):

> Risco é uma combinação de componentes, tais como ameaças, vulnerabilidades e impactos. A análise de riscos engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos, a qual identifica os componentes críticos e o custo potencial ao usuário do sistema.

A análise de riscos é um dos motrizes das políticas da segurança da informação das organizações. Conforme Moreira (2001, p. 11):

Como é impossível prever com exatidão em termos de variedade e freqüência os inúmeros acontecimentos que poderão ocorrer, este tipo de análise nos aponta os possíveis perigos e suas conseqüências em virtude das vulnerabilidades presentes no ambiente computacional de muitas empresas.

Sob a perspectiva da análise de riscos de uma organização, é possível identificar as diversas nuances da segurança da informação. Pode-se, por exemplo, perceber que, em aspectos de segurança física, a organização está bem posicionada, mas em contrapartida, deixa muito a desejar no que tange à segurança lógica de seus sistemas. Dessa forma pode-se avaliar a segurança da informação sob diferentes prismas tais como: segurança física e segurança lógica.

Nesse contexto, Ferreira (2003, p. 130) diz que "[...] o primeiro passo a ser tomado para investir em segurança física deve ser a realização de uma análise dos riscos e vulnerabilidades físicas que a organização possa estar exposta".

A segurança física, não menos importante que a segurança lógica, prevê uma série de procedimentos e controles relativos ao ambiente e aos ativos, principalmente os físicos, que garantam os pilares da segurança da informação. Sem um maior aprofundamento sobre o tema, o que pode ser analisado em relação à segurança física são fatores como o *backup* dos dados e toda sua manipulação, armazenamento e descarte; controle de acesso físico à sala dos servidores computacionais, provimento de redundância elétrica para os equipamentos de tecnologia, processos de entrada e saída de equipamentos da organização, condições do cabeamento e condições ambientais do local onde se encontram os ativos, dentre outros (MOREIRA, 2001).

Adicionalmente, Ferreira (2003, p. 128) diz que:

> Os equipamentos devem ser fisicamente protegidos contra ameaças à sua segurança e perigos ambientais. A proteção dos equipamentos, incluindo aqueles utilizados fora das instalações físicas da organização [...] é necessária para reduzir o risco de acessos não autorizados a dados e para proteção contra perda ou danos.

Afora a visão de acessos não autorizados, perda ou danos, é importante salientar que a simples retirada de um serviço do ar impacta diretamente no pilar "disponibilidade" e causa um incidente de segurança e prejuízos à organização.

Acessos físicos não autorizados e incidentes procedentes de causas naturais também estão relacionados à segurança física do ambiente. Dias (2000, p. 100) sobre essa abordagem diz: "A segurança física pode ser abordada de duas formas: segurança de acesso, que trata das medidas de proteção contra acesso físico não autorizado e segurança ambiental, que trata da prevenção de danos por causas naturais".

Qualquer acesso às dependências da organização, desde áreas de trabalho até os centros de processamento de dados, bibliotecas de manuais e mídias de *software*, dentre outros, deve ser controlado, por meio de formalização, para que o acesso seja realizado apenas por funcionários autorizados (FERREIRA; ARAÚJO, 2006).

Conforme Dias (2000, p. 104), os controles ambientais "[...] visam proteger os recursos computacionais contra danos provocados por desastres naturais (incên-

dios, enchentes), por falhas na rede de fornecimento de energia, ou no sistema de ar condicionado, por exemplo".

Pode-se perceber que não se trata apenas de tecnologia ou de controles providos apenas pela área de tecnologia, mas, indubitavelmente, são controles e procedimentos administrativos que envolvem diversas áreas e que devem ou deveriam ser parte integrante da cultura da organização.

Os controles de acesso lógico devem abranger o recurso tecnológico o qual se pretende proteger e o usuário a quem se pretende fornecer determinados privilégios e acessos. O controle de acesso lógico pode ser resumido em termos de funções de identificação e autenticação de usuários, gestão de privilégios, com concessão e revogação e na prevenção de acessos não autorizados (FERREIRA, 2003).

Sobre a segurança lógica, Dias (2000, p. 84) diz:

> O acesso lógico nada mais é que um processo em que um sujeito ativo deseja acessar um objeto passivo. O sujeito normalmente é um usuário ou um processo, e o objeto pode ser um arquivo ou outros recursos como memória ou impressora. Os controles de acesso lógico são, então, um conjunto de medidas e procedimentos, adotados pela organização ou intrínsecos aos softwares utilizados, cujo objetivo é proteger dados, programas e sistemas contra tentativas de acesso não autorizado [...]. O compartilhamento de senhas, o descuido na proteção de informações confidenciais ou a escolha de senhas facilmente descobertas, por exemplo, pode comprometer a segurança das informações.

A segurança lógica, portanto, vai além de controle de acessos e permissões de usuários em sistemas, ela também abrange cultura dos funcionários em relação ao uso de senhas de sistemas e procedimentos, muitas vezes simples, que podem evitar incidentes de segurança.

Mesmo com todos esses controles, com a implantação da política e uma mudança cultural na organização, podem ocorrer situações de força maior que causem sinistros ou até mesmo a parada total das atividades da empresa. O Plano de Continuidade de Negócios, doravante denominado PCN, entra em ação quando ocorrem situações extremas que causam grandes danos aos negócios. Esse é um longo tópico dentro das disciplinas de Segurança da Informação e nos remete a palavras como contingência e continuidade. Para Sêmola (2003, p. 98), o PCN visa:

> [...] garantir a continuidade de processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre". O mesmo autor exemplifica de forma descontraída que o PCN "[...] deve ser eficaz como o pára-quedas reserva em momento de falha principal, garantindo, apesar do susto, a vida do pára-quedista em queda.

Porém, um Plano de Continuidade de Negócios não tem um viés milagroso; ele visa manter o negócio vivo, mas isso não quer dizer que o mantenha vivo e totalmente funcional. Em caso de sinistros, esse tipo de planejamento deverá manter em níveis aceitáveis os principais processos de negócio (FERREIRA, 2003).

Suponha que o Instituto Nacional do Seguro Social (INSS), quando ocorrido o fatídico incêndio em 2005, tivesse um Plano de Continuidade de Negócios instituído. Certamente as atividades teriam sido interrompidas por menos tempo, haveria menos processos destruídos porque, provavelmente, existiria contingenciamento dos dados e o transtorno para a sociedade seria menor. Quando se fala nos atentados terroristas do 11 de Setembro nos Estados Unidos da América, clássico exemplo do meio acadêmico, não há como mensurar quantas empresas foram à falência por não terem um PCN ou por terem um PCN que envolvia a continuidade das operações muito próximas ao local do acidente e que por isso também foram destruídas, como, por exemplo, *datacenters,* redundantes na segunda torre.

De acordo com Ferreira (2003, p. 86), os principais objetivos do Plano de Continuidade de Negócios são:

> Garantir a segurança dos empregados e visitantes;
>
> Minimizar danos imediatos e perdas numa situação de emergência;
>
> Assegurar a restauração das atividades, instalações e equipamentos o mais rápido possível;
>
> Assegurar a rápida ativação dos processos de negócio críticos;
>
> Fornecer conscientização e treinamento para as pessoas-chave encarregadas desta atividade.

Conclusivamente, todo o universo de segurança da informação é amparado por normas e melhores práticas vigentes no mercado. Alguns organismos como o *International Organization for Standardization* (ISO), o *National Institute of Standards and Technology* (NIST), o *IT Governance Institute* e a *Information Systems Audit and Control Association* (ISACA) desenvolveram metodologias e melhores práticas em segurança da informação que

são reconhecidas em um contexto mundial e largamente utilizadas (FERREIRA; ARAÚJO, 2006).

Das metodologias e melhores práticas citadas anteriormente, as mais difundidas são o Cobit da ISACA e a ISO 17799, que, após atualizações, tornou-se ISO 27001. Para Alves (2006, p. 29):

> O Cobit possui uma flexibilidade de atuação com outras normas e metodologias que outros padrões não possuem. Além disso, sua comunicação com os objetivos de negócio é muito clara, o que permite realizar a integração de TI ao negócio de forma simples.

A norma ISO 17799 é originária da norma britânica British Standard (BS) 7799 e foi traduzida e disponibilizada pela Associação Brasileira de Normas Técnicas (ABNT). De forma geral, esta ISO define um código de práticas para gestão de segurança da informação contando com 10 domínios reunidos em 36 grupos que se desdobram em um total de 27 controles (SÊMOLA, 2003).

2.5 Governança, aspectos legais e conformidade

A segurança da informação já deixou de ter um viés meramente sugestivo, em termos de boas práticas, tornando-se essencial e, por muitas vezes, obrigatória em algumas organizações. Seja por força de leis, decretos ou por regulações do próprio mercado que clamam por conformidade na adoção de procedimentos de segurança. Esses procedimentos muitas vezes estão inclusos em uma série de premissas envoltas em um contexto de Governança Corporativa. Governança é diferente de governar: a Governança Corporativa tem muito a ver com prestação de contas, transparência e responsabilidade corporativa, enquanto governar é fazer uso da batuta do poder, sem necessariamente garantia de sucesso (ALVES, 2006).

Escândalos recentes da economia americana com a falsificação de informações como demonstrações contábeis, envolvendo, inclusive, grandes empresas de auditoria do mundo, ocasionaram uma perda de confiança sucessiva por parte de acionistas, principalmente daqueles que investiam em ações. Após a ocorrência desses acontecimentos, uma série de normas passou a vigorar, a exemplo da lei americana *Sarbanes Oxley* (SOX) de 2002, de forma a garantir confiabilidade e disponibilidade dos sistemas e aplicativos que indiquem a situação da organização no momento em que são acessados (ALVES, 2006). Exemplificativamente, uma empresa que pretende abrir seu capital e figurar em bolsas de valores internacionais deve se adaptar a uma série de procedimentos ou normas que muitas vezes envolvem aspectos de segurança da informação. Em um resumido artigo da web intitulado "O que é a lei *Sarbannes-Oxley* e quais os impactos na TI", Costa (2006, p. 2) cita que a lei "[...] visa garantir a transparência na gestão financeira das organizações, credibilidade na contabilidade, auditoria e a segurança das informações para que sejam realmente confiáveis, evitando assim fraudes, fuga de investidores [...]".

Ainda sobre a SOX, Pinheiro (2009, p. 200) afirma:

> A base para a implementação está na área de TI, pois cerca de 90% dos processos de negócio são controlados por TI. Dessa forma, esse departamento não só será responsável pelo controle de acesso, dados e guarda de históricos, como também terá de autenticar cada passo em cada processo.

A partir do momento em que se fala de auditoria, segurança das informações e fuga de investidores, claramente causadas por desconfiança ou descredibilidade da empresa perante o mercado, há uma referência direta a aspectos de segurança da informação. Dentro desse contexto, tem-se a Governança de TI e de Segurança que funcionarão como habilitadores responsáveis pela criação de processos amplamente controlados e alinhados com a estratégia da empresa e com as regulações setoriais ou mercadológicas.

Em uma perspectiva governamental, há uma série de incentivos, iniciativas, propagandas, decretos, manuais, instruções normativas e até leis voltadas à conformidade e segurança das informações. Os órgãos não podem mais simplesmente postergar um debate mais profundo sobre o tema. Em seu livro "Direito Digital", Pinheiro (2009, p. 216) diz:

> É inegável que o formato digital promove maior visibilidade, o que possibilita, indiretamente, maior transparência e controle da sociedade sobre aquilo que está sendo feito pelo ente público. No entanto, as mesmas preocupações quanto à segurança e a documentação eletrônica adequada das operações do setor privado devem ser tomadas também pelo setor público.

Não é objetivo deste artigo descrever detalhadamente todas as leis voltadas à conformidade em Segurança da Informação na esfera do governo, portanto serão citadas as mais relevantes.

Na Constituição Federal existem diversos aspectos ligados à segurança das informações, direta ou indireta-

mente. O artigo 5º, inciso XXXIII e o art. 37, § 3º, inciso II, por exemplo, têm como mandamento legal o direito às informações e ao acesso aos registros públicos; logo, o preceito de segurança da informação é o da disponibilidade das informações constantes nos órgãos públicos. Os artigos 23, incisos III e IV e 216, § 2º, cujos mandamentos legais são o dever do Estado de proteger os documentos e obras, e a obrigação da Administração Pública de promover a gestão documental, respectivamente, versam sobre proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.

Há mais de 10 anos, o Decreto nº 3.505 de 13 de junho de 2000, da Presidência da República, instituía a Política de Segurança da Informação nos órgãos e entidade da Administração Pública Federal. Esse Decreto possui uma série de direcionamentos que envolvem desde a elaboração de uma POSIC seguida de uma série de diretrizes de conformidade com a política estabelecida. Não se trata de recomendações, mas de obrigatoriedade e de conformidade. Certamente, o Decreto enfoca também conscientização, programas de capacitação, divulgação e até a instituição de um comitê para auxiliar os demais órgãos a alcançarem esse objetivo.

Esse Decreto também fala em conformidade dos órgãos para o alcance dos objetivos da segurança da informação, a saber:

> Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:
>
> **I - Certificado de conformidade:** garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal;
>
> Art. 3º São objetivos da Política da Informação:
>
> I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis (BRASIL, 2000, grifo nosso).

O artigo 6º da Lei nº 10.683, de 28 de maio de 2003 atribui, dentre outros, à competência do Gabinete de Segurança da Informação da Presidência da República de "[...] coordenar as atividades de inteligência federal e de segurança da informação" (BRASIL, 2003).

O Decreto nº 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. Nesse Decreto, em seu artigo 3º, tem-se o seguinte:

> Parágrafo único. Toda autoridade responsável pelo trato de dados ou informações sigilosos providenciará para que o pessoal sob suas ordens conheça integralmente as medidas de segurança estabelecidas, zelando pelo seu fiel cumprimento.

Dessa forma, fica clara a responsabilidade do agente público pelo manuseio de informações no âmbito da Administração Pública.

A Instrução Normativa GSI nº 1, de 13 de junho de 2008, disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Afora as atribuições de acompanhamento, fiscalização e orientação do GSI, é interessante ressaltar o artigo 5º, que fala sobre as competências dos demais órgão da Administração Pública Federal, direta e indireta:

I - coordenar as ações de segurança da informação e comunicações;

II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Comunicações;

VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações; e

VIII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI.

Ressalte-se, ainda, que existe uma série de normas complementares para darem apoio ferramental e metodológico aos mecanismos legais de segurança da

informação. Por exemplo, a Norma Complementar nº 02/IN01/DSIC/GSIPR aborda a metodologia de Gestão de Segurança da Informação e Comunicações, a Norma Complementar nº 03/IN01/DSIC/GSIPR versa sobre diretrizes para a elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal, dentre diversas outras que podem ser acessadas no próprio sítio do Departamento de Segurança das Informações (DSIC) da Presidência da República. No Anexo II deste artigo, existe um quadro de autoria da Dra. Tatiana Malta Vieira, Procuradora Federal da Advocacia-Geral da União, disponibilizado no sítio do DSIC, com uma série de legislações específicas relacionadas à Segurança da Informação e Comunicações.

Percebe-se que, tanto na esfera pública quanto na privada, há a necessidade de conformidade com boas práticas – normativos e leis que darão suporte às estratégias de governança institucional – dos negócios que darão subsídio para uma boa prestação de serviços, com qualidade e segurança.

3 Análise e considerações finais

Esta análise final dar-se-á em dois contextos: o primeiro pela observação das estruturas do Ministério do Desenvolvimento Agrário e dos demais ministérios, salvo as exceções; o segundo, pela análise dos resultados da coleta de dados obtida por meio do questionário aplicado aos colaboradores.

Percebe-se grande dificuldade na implantação de políticas de cunho cultural em um ambiente caracterizado por uma subcultura enraizada e de instabilidade, por conta de aspectos externos, de cunho político, eleitoral e orçamentário. É deveras complicado motivar e convencer gestores a aderirem a um plano contínuo sendo que nem suas permanências nos órgãos o são. Porém, as normas voltadas ao Governo Federal estão em voga e há um movimento crescente por parte de alguns órgãos como, o Tribunal de Contas da União, a Controladoria Geral da União, o Gabinete de Segurança Institucional da Presidência da República e o próprio Ministério do Planejamento, Orçamento e Gestão que têm atuado de forma vanguardista, até pela maturidade de suas estruturas e corpo funcional e estratégico, ou por características intrínsecas às suas atribuições na estimulação e na exigência de procedimentos de governança e segurança das informações.

O fato é que a necessidade de conformidade está aumentando a cada dia e o Governo não pode mais postergar esse fato. Uma notícia amplamente veiculada em sítios da internet mostrou que, segundo um relatório aprovado pelo Tribunal de Contas da União (TCU), em outubro de 2010, 65% dos órgãos da administração pública federal não possuíam política corporativa de segurança da informação. De acordo com o levantamento, a situação é "preocupante" e não foi notada evolução na área, em relação a outro estudo feito em 2007.[21] No MDA, acaba de ser publicada a Política de Segurança da Informação, elaborada na Coordenação Geral de Modernização e Informática e aprovada por uma série de secretarias, incluindo a Secretaria Executiva e o Gabinete do Ministro. Inclusive as áreas de TI das demais secretarias foram envolvidas. A partir de agora, é necessário que se inicie um processo de mudança cultural para que ela possa ser implantada e não acabe no esquecimento.

No *livro - case*, "Governança para Resultados no Ministério da Saúde", Bassit, Blumm e Martins (2009, p. 30), numa perspectiva similar, afirmam o seguinte:

> Uma boa gestão é aquela que alcança resultados. E isso, no setor público, significa atender às demandas, aos interesses e às expectativas dos beneficiários, sejam cidadãos ou organizações, criando valor público. Resultados não acontecem por acaso. Governos em geral, organizações públicas, políticas, programas e projetos não são auto-orientados para resultados. Também não basta apenas defini-los bem, pois resultados não são auto-executáveis, a implementação segue sendo a grande variável crítica.

Contextualizando com o cotidiano, principalmente da Tecnologia da Informação, é necessário, para que se chegue ao alcance do objetivo, além de uma mudança de cultura, uma mudança estrutural, que já dá sinais de começar no MDA. Primeiramente, para que a execução da política tenha êxito, as áreas de Tecnologia da Informação, antes descentralizadas e autônomas, devem ficar sob a tutela da CGMI. Os sistemas, que manipulam informações críticas e milhares de dados e arquivos por dia, devem estar centralizados em uma infraestrutura única, segura e moderna, com gestão centralizada e com premissas de acesso bem definidas. Isso porque a política de segurança da informação vem amparada por normas complementares para cada abordagem da SI como segu-

[2] A matéria pode ser vista em: <http://www.egov.ufsc.br/portal/>.

rança física, segurança lógica, política de acessos, políticas de salvaguarda de dados e, sem essa adequação, não haverá sustentação à política.

Caso isto não ocorra, a política de segurança da informação não terá validade, pois logo que alguém tiver um interesse ferido por algum ponto do normativo, como não há subordinação à CGMI e há uma ligação aos níveis estratégicos da organização, haverá um atravessamento do fluxo e as áreas demandarão direto ao gabinete, por exemplo. Como a CGMI está abaixo da Secretaria Executiva, até que se possa tomar alguma providência, a burocracia e o tempo já tornam inviável a interferência em um processo que cause um risco, por exemplo.

Sugere-se, a exemplo do Ministério do Planejamento, Orçamento e Gestão (MPOG), a criação de uma Secretaria de Tecnologia da Informação e Logística ligada diretamente ao Ministro. Isto proveria força política na organização para levar adiante ideias, campanhas, políticas e programas relativos à governança corporativa, envolvendo diretamente a implantação da política em segurança das informações.

Das respostas dos questionários, pôde se observar que os servidores em especial estão mais preocupados com as diretrizes de segurança da informação e o futuro da organização do que os demais colaboradores, o que é facilmente compreensível em função de seu vínculo permanente. Tornou-se claro, após as análises, que falta muito em termos de comunicação interna, educação e treinamentos dos colaboradores, haja vista o entendimento precário que a grande maioria demonstrou em relação a procedimentos e conceitos simples de segurança da informação. De forma mais ampla, quando questionados se tinham conhecimento sobre algum simples normativo relacionado à informática, 57% responderam que não tinham qualquer conhecimento. Para muitos colaboradores, não estão claros os objetivos e vantagens da segurança da informação; ou demonstram desconhecimento ou enxergam apenas sua desvantagem. Em relação a isso, apenas 26% afirmaram perceber as ações e procedimentos de segurança da informação de forma positiva.

Sabe-se que segurança da informação é um assunto que deve estar sedimentado em todos os colaboradores de uma organização. Dessa forma, recomenda-se a criação de campanhas de conscientização, disseminadas a partir de pontos focais, ou pessoas-chave, dentro de departamentos, para que atinjam também os colaboradores sem vínculo permanente.

Complementarmente, há a necessidade de uma política de comunicação interna em nível de informativos e propaganda sobre a importância que a política de segurança das informações tem para o cotidiano dos funcionários e para as atividades fim do órgão. Já foi dito que a comunicação é um dos principais elementos do processo de mudança, portanto, é extremamente válida a conscientização de todo corpo funcional sobre procedimentos e boas práticas de segurança da informação.

Percebeu-se que grande parte dos entrevistados acredita que a segurança da informação seja importante em sua rotina de trabalho, com 65% do total de respondentes, e boa parte deles disse aceitar os procedimentos de segurança aplicados no âmbito do Ministério, com 41% do total. Outra parcela considerável da amostra, 56%, respondeu que estaria disposta a mobilizar suas equipes ao cumprimento de procedimentos e boas práticas e crê que essa é uma responsabilidade de toda a organização.

Porém, na última questão, a maioria julgou que o órgão não poderia ter em sua estrutura uma política de segurança das informações aplicada de forma efetiva e o resultado mostrou um pouco dessa percepção que se combina com os resultados da primeira análise desta conclusão: falta de centralização das informações, servidores utilizando infraestrutura precária de terceiros, falta de comunicação, conhecimentos, treinamentos, difícil acesso à informação e falta de pessoal capacitado.

Conclusivamente, percebe-se que o Ministério do Desenvolvimento Agrário está parcialmente apto, com iniciativas isoladas, a implementar sua política de segurança da informação; porém, primeiramente, deve cumprir uma etapa de mudanças que não são de cunho técnico ou tecnológico, mas em sua estrutura interna, em sua gestão e cultura.

Para trabalhos futuros, propõe-se um estudo de gerenciamento de mudança organizacional com foco em governança corporativa e processos bem definidos, pois, acredita-se que essa é a chave para se implantar qualquer tipo de política.

Referências

ALBUQUERQUE, R.; RIBEIRO, B. *Segurança no desenvolvimento de software*. Rio de Janeiro: Campus, 2002.

ALVES, G. A. *Segurança da informação*: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna, 2006.

AKTOUF, O. O simbolismo e a cultura de organização: dos abusos conceituais às lições empíricas. In: CHANLAT, J. F. (Org.). *O indivíduo nas organizações:* dimensões esquecidas. São Paulo: Atlas, 1994. v. 2, p. 39-79.

BEER, M. *Gerenciando mudança e transição*. Trad. Managing Change and Transition. Rio de Janeiro: Record, 2010.

BRASIL. *Decreto n° 7.280, de 31 de agosto de 2010*. Altera o início da vigência do Decreto nº 7.255, de 4 agosto de 2010, que aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções.s Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7280.htm>. Acesso em: 04 abr. 2011.

BRASIL. *Decreto nº 7.255, de 4 de agosto de 2010*. Aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções gratificadas do Ministério do Desenvolvimento Agrário, e dá outras providências. Disponível em: <http://www.jusbrasil.com.br/legislacao>. Acesso em: 31 jan. 2011.

BRASIL. *Lei nº 10.683, de 28 de maio de 2003*. Dispõe sobre a organização da presidência da república e dos ministérios, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2003/L10.683.htm>. Acesso em: 02 fev. 2011.

BRASIL. *Gratificadas do ministério do desenvolvimento agrário*. Disponível em: <http://www.jusbrasil.com.br/legislacao>. Acesso em: 31 jan. 2011.

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

CARBONE, P. P. Cultura organizacional no setor público brasileiro: desenvolvendo uma metodologia de gerenciamento da cultura. *Revista de Administração Pública*, Rio de Janeiro, v. 34, n. 2, p. 133-144, mar./abr. 2000.

CERTO, Samuel C. *Administração moderna.* São Paulo: Pearson Brasil, 2003.

CERVO, A. R.; BERVIAN, P. A. *Metodologia científica***.** 5. ed. São Paulo: Prentice Hall, 2002.

COSTA, Imasters L. *O que é a lei Sarbannes-Oxley e quais os impactos na TI*. 2006. Disponível em: <http://imasters.com.br/artigo/5096/direito/o_que_e_lei_sarbanesoxley_e_quais_os_impactos_na_ti/>. Acesso em: 12 mar. 2011.

CHIAVENATO, Idalberto. *Administração nos novos tempos.* 2. ed. Rio de Janeiro: Elsevier, 2005.

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

FERREIRA, F. N. F.; ARAÚJO, M. T. *Política de segurança da informação***:** guia prático para implementação e elaboração. Rio de Janeiro: Ciência Moderna, 2006.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. *Information security governance***:** guidance for boards of directors and executive management. Illinois: Rolling Meadows, 2001.

KANAANE, R. *Comportamento humano nas organizações:* o homem rumo ao século XXI. 2. ed. São Paulo: Atlas, 1999.

KOTLER, Philip; ARMSTRONG, Gary. *Princípios de marketing.* 9. ed. São Paulo: Pearson Prentice Hall, 2007.

MARCONI, M. A.; LAKATOS, E. M. *Técnicas de pesquisa.* 7. ed. São Paulo: Atlas, 2008.

MOTTA, F. C. P.; CALDAS, M. P. *Cultura organizacional e cultura brasileira.* São Paulo: Atlas, 1997.

MOREIRA, Nilton S. *Segurança mínima*. Rio de Janeiro: Axcel, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001:2006*: tecnologia da informação: sistema de gestão da segurança da informação. Rio de Janeiro, 2006.

PECK, Patrícia Pinheiro. *Direito digital***.** São Paulo: Saraiva, 2009

PEIXOTO, Mario C. P. *Engenharia social e segurança da informação na gestão corporativa*. Rio de Janeiro: Brasport, 2006.

PIRES, J. C. S.; MACEDO, K. B. Cultura organizacional em organizações públicas no Brasil. *Revista de Administração Pública***.** Rio de Janeiro, v. 40, n.1, p.81-105, jan./fev. 2006.

ROBBINS, Stephen P. *Comportamento organizacional.* São Paulo: Prentice Hall, 2002.

SEMOLA, M. *Gestão da segurança da informação***.** Rio de Janeiro: Campus, 2003.

SILVA, L. P.; FADUL, E. M. C. *Cultura organizacional em organização pública***:** as bases da mudança organizacional a partir da reforma gerencial. In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA**,** 7., 2007. Disponível em: <http://www.aedb.br/seget/artigos07/1437_1437_Cultura%20organizacional%20em%20organizacoes%20publicas.pdf>. Acesso em: 27 fev. 2011.

SILVA, P. T.; CARVALHO, H.; TORRES, C. B. *Segurança dos sistemas de informação*: gestão estratégica da segurança empresarial. Portugal: Centro Atlântico, 2003.

VERGARA, Sylvia Constant. *Métodos de pesquisa em administração*. São Paulo: Atlas, 2007.

ANEXO A– Questionário

Prezado colaborador,

Este questionário tem por objetivo mensurar a percepção de aspectos voltados a segurança da informação no âmbito do Ministério do Desenvolvimento Agrário. Não há a necessidade de identificação.

Para um maior entendimento do assunto abordado, é importante conceituar:

'Segurança da informação' está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança em Informática está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas, localidades que comportam dados confidenciais, controles ambientais e até pessoas.

Por favor, informe seu vínculo com o MDA:

( ) Servidor

( ) Consultor

( ) Terceirizado

01) Você tem conhecimento de algum normativo/ recomendações do MDA voltados a informática?

( ) SIM

( ) NÃO

02) Como tomou conhecimento desse(s) normativo(s) / recomendação?

( ) Treinamento específico

( ) Comunicados internos

( ) Documentos disponíveis na intranet

( ) Pelos colegas

( ) Por sua chefia

( ) Por meio de incidentes de segurança

03) Dos aspectos a seguir, qual você considera mais importante em termos de segurança institucional:

( ) Manipulação de informações críticas

( ) Segurança física do ambiente de trabalho

( ) Acesso não autorizado de pessoas à ambientes do MDA

( ) Conteúdo digital sobre o MDA

04) Dos itens a seguir, sobre quais você tem um maior conhecimento sobre procedimentos de segurança da informação?

( ) Definição de acesso a sistemas

( ) Utilização de e mail

( ) Utilização de internet

( ) Utilização de computadores

( ) Uso das informações institucionais

( ) Realização de Backup's

( ) Instalação de software's

( ) Uso de senhas

( ) Nenhuma

05) Se você se depara com uma situação em que desejar realizar algum tipo de atividade relacionada à informática e é bloqueado(a) com a premissa de impacto na segurança das informações, você:

( ) Entende e aceita.

( ) Questiona e tenta justificar.

( ) Busca maneiras de fazer mesmo assim.

( ) Busca apoio de sua chefia ou de níveis superiores.

06) Classifique em que medida considera que segurança da informação é ou pode ser importante para suas atividades profissionais? (1 para pouco e 6 para muito)

( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5 ( ) 6

07) Você acredita que procedimentos voltados à Segurança da Informação impactam positiva ou negativamente no seu trabalho?

( ) Negativamente

( ) Positivamente

08) Na sua percepção, como os funcionários do MDA entendem as ações e procedimentos de Segurança da Informação?

( ) De forma positiva

( ) De forma negativa

( ) De forma desconfiada

( ) Não acreditam que possa trazer benefício

( ) Não tenho opinião

( ) Outros: _____

09) Você acredita que a área de segurança da informação é de competência:

( ) Das áreas técnicas

( ) Das áreas gestoras

( ) De toda a organização

10) Em relação ao comprometimento das equipes e adoção de mudanças orientadas pela área de segurança:

( ) Acredito que as coisas devam ser feitas da forma que sempre deram certo.

( ) Mobilizo meu pessoal para adequação às novas regras e procedimentos.

( ) Ignoro e procuro saber apenas quando for de meu interesse.

11) Você já teve alguma experiência com incidentes de segurança da informação dentro do MDA (ex: e-mail's solicitando senha, acesso não autorizado a documentos ou sistemas, uso de informações privilegiadas por pessoas não autorizadas, dentre outros.)?

( ) SIM

( ) NÃO

12) Você acredita que a estrutura oferecida pelo ministério permite a implantação de uma política de segurança da informação de forma eficiente? Caso não, exponha o motivo.

( ) SIM

( ) NÃO _____

ANEXO B – QUADRO DE LEGISLAÇÕES SOBRE SEGURANÇA DA INFORMAÇÃO

Quadro da legislação específica de caráter federal relacionada à segurança da informação[3]

Regulamento	Assunto
Lei nº 7.232, de 29 de outubro de 1984.	Dispõe sobre a Política Nacional de Informática, e dá outras providências.
Lei nº 8.248, de 23 de outubro de 1991.	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
Lei nº 9.296, de 24 de julho de 1996.	Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.
Lei nº 9.472, de 16 de julho de 1997.	Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.
Lei nº 9.507, de 12 de novembro de 1997.	Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.

3 Esta compilação é um trabalho da Dra Tatiana Malta Vieira - Procuradora Federal da Advocacia Geral da União. Disponível em <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>

Regulamento	Assunto
Lei nº 9.609, de 19 de fevereiro de 1998.	Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Lei nº 9.883, de 07 de dezembro de 1999.	Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.
Lei nº 8.159/91, de 08 de janeiro de 2001.	Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.
Lei Complementar 105, de 10 de janeiro de 2001.	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
Medida Provisória nº 2.200-2, de 24 de agosto de 2001.	Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.
Lei nº 10.973, de 02 de dezembro de 2004.	Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.
Lei nº 11.111, de 05 de maio de 2005.	Regula o direito à informação e ao acesso aos registros públicos.
Lei nº 11.419, de 19 de dezembro de 2006.	Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.
Decreto nº 2.295, 04 de agosto de 1997.	Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.
Decreto nº 2.556, de 20 de abril de 1998.	Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Decreto nº 3.294, de 15 de dezembro de 1999.	Institui Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.
Decreto nº 3.505, de 13 de junho de 2000.	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto de 18 de outubro de 2000.	Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.
Decreto nº 3.714, 03 de janeiro de 2001.	Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto nº 2.954, de 29 de janeiro de 1999, e dá outras providências.
Decreto nº 3.996, de 31 de outubro de 2001.	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
Decreto nº 4.073, de 03 de janeiro de 2002.	Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.
Decreto nº 4.376, de 13 de setembro de 2002.	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.
Decreto nº 4.522, 17 de dezembro de 2002.	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.

Regulamento	Assunto
Decreto nº 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.
Decreto nº 4.689, de 07 de maio de 2003.	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação – ITI, e dá outras providências.
Decreto nº 4.829, de 03 de setembro de 2003.	Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
Decreto de 29 de outubro de 2003.	Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências.
Decreto nº 5.301, de 09 de dezembro de 2004.	Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.
Decreto nº 5.450, de 31 de maio de 2005.	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto nº 5.563, de 11 de outubro de 2005.	Regulamenta a Lei nº 10.973, de 02/12/04, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências.
Decreto nº 5.584, de 18 de novembro de 2005.	Dispõe sobre o recolhimento ao Arquivo Nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN.
Decreto nº 5.772, de 08 de maio de 2006, art. 8º.	Institui na estrutura regimental do Gabinete de Segurança Institucional da Presidência da República o Departamento de Segurança da Informação e Comunicações com diversas atribuições na área de segurança da informação e comunicações.
Decreto nº 6.605, de 14 de outubro de 2008.	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.
Instrução Normativa nº 1 do GSI, de 13 de junho de 2008.	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Resolução nº 58 do INPI, de 14 de julho de 1998.	Estabelece normas e procedimentos relativos ao registro de programas de computador.
Resolução nº 59 do INPI, de 14 de julho de 1998.	Estabelece os valores das retribuições pelos serviços de registro de programas de computador.
Resolução nº 338 do STF, de 11 de abril de 2007.	Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF.
Resolução nº 140 do TST, de 13 de setembro de 2007.	Regulamenta, no âmbito da Justiça do Trabalho, a Lei n° 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.
Resolução nº 22.718/08 do TSE, arts. 18 e 19.	Regula a propaganda eleitoral na internet em campanha nas eleições de 2008.

Para publicar na revista Universitas Gestão e TI,
entre no endereço eletrônico
www.publicacoesacademicas.uniceub.br.
Observe as normas de publicação, facilitando e agilizando o trabalho de edição.