Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

EDUARDO CAMARGOS LAGARES DO NASCIMENTO

FATORES ESTRUTURAIS E CULTURAIS QUE IMPACTAM NA IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO MINISTÉRIO DA JUSTIÇA

Brasília
2014

EDUARDO CAMARGOS LAGARES DO NASCIMENTO

FATORES ESTRUTURAIS E CULTURAIS QUE IMPACTAM NA IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO MINISTÉRIO DA JUSTIÇA

Monografia apresentada ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-Graduação Lato Sensu em Governança em Tecnologia da Informação

Orientador: Prof. Dr. Maurício Rocha Lyra

Brasília
2014

EDUARDO CAMARGOS LAGARES DO NASCIMENTO

FATORES ESTRUTURAIS E CULTURAIS QUE IMPACTAM NA IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO MINISTÉRIO DA JUSTIÇA

Monografia apresentada ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-Graduação Lato Sensu em Governança em Tecnologia da Informação

Orientador: Prof. Dr. Maurício Rocha Lyra

Brasília/DF, 25 de outubro de 2014.

Banca Examinadora

_____

Prof. Dr. Nome completo

_____

Prof. Dr. Nome completo

AGRADECIMENTOS

Agradeço ao orientador Maurício Lyra pela paciência e perseverança em me orientar apesar das adversidades de tempo que enfrentei, a Michel Gomes Nogueira do Ministério da Justiça pela contribuição e boa vontade no alcance dos objetivos desse trabalho e aos meus pais pelo apoio incondicional e inspiração.

A maior recompensa do ser humano é que, enquanto os animais sobrevivem ajustando-se ao meio em que vivem, o homem sobrevive ajustando a si próprio." Ayn Rand

RESUMO

As características de cultura e estrutura organizacionais na Administração Publica Federal são fatores que desafiam a implantação de fato de uma política de segurança da informação em suas organizações. Ao considerar aspectos culturais e de estrutura organizacional pôde-se identificar o quão complexo é implantar controles relativos à segurança da informação, dado o impacto proveniente dos fatores de influência. A fim de detectar esses fatores, realizou-se uma análise sob essas perspectivas e observou-se uma série de resultados que influenciam diretamente na aplicação efetiva de controles baseados numa política de segurança da informação, utilizando como objeto de pesquisa o Ministério da Justiça. Uma vez que a política de segurança da informação é um requisito legal para organizações da administração pública federal e possuem uma importância real para a sociedade, o fato de que elas desempenham um papel meramente de conformidade, sem uma aplicação prática e controlada, implica a não efetividade da iniciativa invocando a necessidade de uma análise mais profunda e proposição de novas ideias sobre o tema.

Palavras-chave: Segurança da informação. Cultura organizacional. Administração Pública Federal

ABSTRACT

The characteristics of cultural aspects and organizational structure in the Brazilian Federal Public Administration are factors that challenge the real implementation of a policy of information security in their organizations. When considering cultural and organizational structure perspectives it was possible identify how complex it is to implement controls related to information security due to the impact from these influencing factors. In order to identify these factors, a analysis was performed under these two perspectives and was observed a series of results that directly influence the effective implementation of controls based on an information security policy using as research object the Ministry of Justice. Once the information security policy is a legal requirement for the federal public administration organizations and have a real importance to society, the fact that they play a merely compliance role without a practical and controlled application, implies not effectiveness of the initiative invoking the need for a deeper analysis and propose new ideas on the subject.

KEY WORDS: Information Security. Organizational Culture. Federal Public Administration.

SUMÁRIO

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, dados utilizados por órgãos de controle e fiscalização e muitas informações sobre os contribuintes.

As organizações sofrem ameaças constantes em seus ativos de informação, o que, em caso de incidentes, representa um prejuízo incalculável. A gama de vulnerabilidades em ambientes corporativos voltados principalmente à Tecnologia da Informação transcende as barreiras tecnológicas, uma vez que a cultura organizacional, processos e governança têm sido percebidos como 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 um incidente 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 este tipo de incidente? Quanto tempo levou para que ela recuperasse todos os dados perdidos? Será que ela recuperou dados perdidos? A maioria das organizações governamentais não está preparada para se recuperar no caso de incidentes dessa natureza, apesar de muitas vezes terem instituídas e aprovadas

pelos mais altos escalões, uma política de segurança da informação, além de terem obrigações legais de protegerem esses dados.

Isso ocorre, dentre outros motivos, porque apesar da força de lei que as obriga a ter uma política de segurança da informação, que contemple a disponibilidade, confidencialidade, 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.

Este cenário é um dos grandes desafios de órgãos do Governo Federal Brasileiro. Este artigo pretende identificar os motivos deste desafio numa perspectiva cultural e estrutural – em termos de análise de organograma – utilizando como objeto de pesquisa o Ministério da Justiça. Dessa forma torna-se necessário realizar a seguinte pergunta: quais os fatores, tanto em termos de estrutura quanto culturais, impactam na implantação de uma política de segurança da informação no Ministério da Justiça?

Este artigo estrutura-se da seguinte forma: primeiramente há uma explanação sobre a estrutura do Governo Federal, sobretudo sobre a estrutura do Ministério da Justiça, suas atribuições, análise estrutural por meio de organogramas e estruturas hierárquicas e suas atividades finalísticas para que os valores da organização sejam mensurados. Posteriormente, é exposta a gama de autores que escreveram sobre temas pertinentes a este artigo, formando o referencial teórico, subdividido em subcapítulos por temas macro, tais como segurança da informação, cultura organizacional e conformidade com legislações e boas práticas voltadas a Segurança da Informação. Em seguida vem à consolidação e análise dos dados coletados e do cenário estudado e por fim estão as considerações finais.

JUSTIFICATIVA

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, isto significa o controle sobre projetos, sobre gastos públicos, sobre políticas de governo, a proteção aos dados dos cidadãos, integridade nacional e principalmente pela prestação de um serviço melhor à sociedade. Esta pesquisa se justifica uma vez que é evidente a necessidade abranger e aprofundar a visão sobre papel da segurança da informação nas estruturas governamentais, com o objetivo de identificar se são efetivas e eficazes de fato, e se não forem, quais os fatores que impedem que sejam. A Segurança da Informação no segmento privado é uma realidade há décadas e pode-se perceber um atraso das estruturas do governo em relação a isto, e partindo do pressuposto de valor das informações, sabe-se que envolvem interesses de segurança nacional e desenvolvimento do país.

Do ponto de vista social esta pesquisa é relevante uma vez que a segurança da informação simboliza transparência, auditabilidade, conformidade legal, integridade das informações dos cidadãos e a soberania nacional. Casos recentes de espionagem provenientes dos Estados Unidos da America despertaram um grande interesse popular sobre o tema e uma maior preocupação das autoridades nacionais. Fatos como esse revelam que não só apenas segredos comerciais de grandes companhias estão em risco, mas qualquer informação que trafegue na nuvem da internet.

O tema da pesquisa expande seu impacto social uma vez que o governo federal oferece uma série de serviços *on line*, o que requer disponibilidade, confiabilidade e integridade.

Para o meio acadêmico esta pesquisa justifica-se, pois, apesar de ser um tema atual e bastante em voga, ele é mais explorado dentro de um aspecto meramente tecnológico e majoritariamente na iniciativa privada, havendo uma vasta possibilidade de exploração de aspectos extratecnológicos, uma vez que está comprovado que segurança da informação transcende a área da tecnologia da informação.

Acredita-se que, com o aumento das pesquisas nessa área, seja possível alcançar um grau de maturidade tal que as aplicações in loco nesta seara se tornem mais eficazes.

Numa perspectiva pessoal esta pesquisa torna-se relevante, pois, é a área de atuação do autor que presencia desafios desta ordem em seu cotidiano profissional e também por acreditar, com base em experiências vividas, que a segurança da informação no âmbito do governo federal ainda precise de debates mais profundos e de um urgente amadurecimento. Por fim, para o autor esta pesquisa também se torna relevante por acreditar que a segurança da informação contribui para uma sociedade mais íntegra e para uma melhor gestão pública.

OBJETIVO GERAL

Analisar o impacto dos aspectos culturais e estruturais na implantação de uma política de segurança da informação no âmbito do Ministério da Justiça.

OBJETIVOS ESPECÍFICOS

- Realizar uma análise de organograma da organização a fim de identificar possíveis gargalos na implantação da política de segurança da informação;

- Investigar a percepção dos colaboradores sobre tópicos relacionados ao tema segurança da informação;

METODOLOGIA

A presente pesquisa é um estudo de caso por analisar características de uma instituição bem definida a partir da perspectiva do autor a fim de analisar uma situação específica da organização. De acordo com Gil (2007, p. 54):

> Um estudo de caso pode ser caracterizado como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social. Visa conhecer em profundidade o como e o porquê de uma determinada situação que se supõe ser única em muitos aspectos, procurando descobrir o que há nela de mais essencial e característico. O pesquisador não pretende intervir sobre o objeto a ser estudado, mas revelá-lo tal como ele o percebe.

O método de pesquisa utilizado, quanto aos fins foi descritivo, à medida que estabeleceu relação entre as variáveis estudadas, descrevendo as características ou fenômenos da população estudada (VERGARA, 2007), e quanto aos meios foi 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 no próprio local onde correm os fenômenos ou onde está a população estudada (MARKONI; LAKATOS, 2008).

O universo de pesquisa foi o total de colaboradores conhecidos do Ministério da Justiça, 2.382, e como foi disponibilizado um questionário fechado sem a

obrigatoriedade de respostas, um percentual mínimo de amostra aceitável foi definido como 8% desse universo.

Para fins da análise dos fatores culturais, foram coletados dados por meio de um questionário fechado, composto de 11 questões, aplicado no Ministério da Justiça para servidores efetivos, comissionados, consultores, estagiários e terceirizados de todos os níveis, ou seja, tático, estratégico e operacional. Este 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 uma melhor aceitação do questionário, ele foi disponibilizado por meio de um comunicado digital emitido pelo próprio Ministério da Justiça no período entre 12 de Fevereiro de 2014 e 18 de Fevereiro de 2014. O questionário e o comunicado digital emitido pelo Ministério da Justiça podem ser visualizados no Anexo A.

Para a análise de organograma foi utilizada a pesquisa bibliográfica, quando da análise de organogramas e normativos da organização disponíveis em seu sítio na internet assim como documentos de fontes diversas, como auditorias do TCU e o Plano Diretor de Tecnologia da Informação do Ministério da Justiça.

A análise final dar-se-á em dois contextos: o primeiro pela observação das estruturas do Ministério da Justiça; o segundo, pela análise dos resultados da coleta de dados obtida por meio do questionário aplicado aos colaboradores. No capítulo 1, será exposto o contexto do objeto de pesquisa, com uma exploração das estruturas ministeriais e do Ministério da Justiça. No capítulo 2 está o referencial teórico com a exposição dos assuntos e autores pertinentes à pesquisa e no capítulo 3 estão as análises estrutural e cultural. Finalmente, estão as conclusões desse artigo.

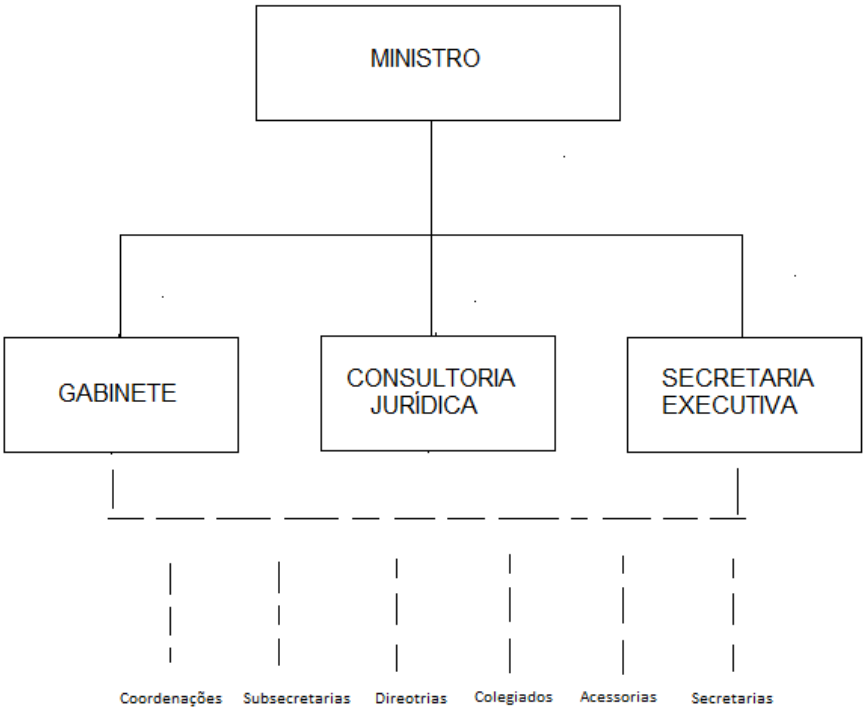
CAPÍTULO 1

1. 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. O Ministério da Justiça, por exemplo, é ligado a Secretaria de Direitos Humanos (SDH) em que seu representante tem o 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:

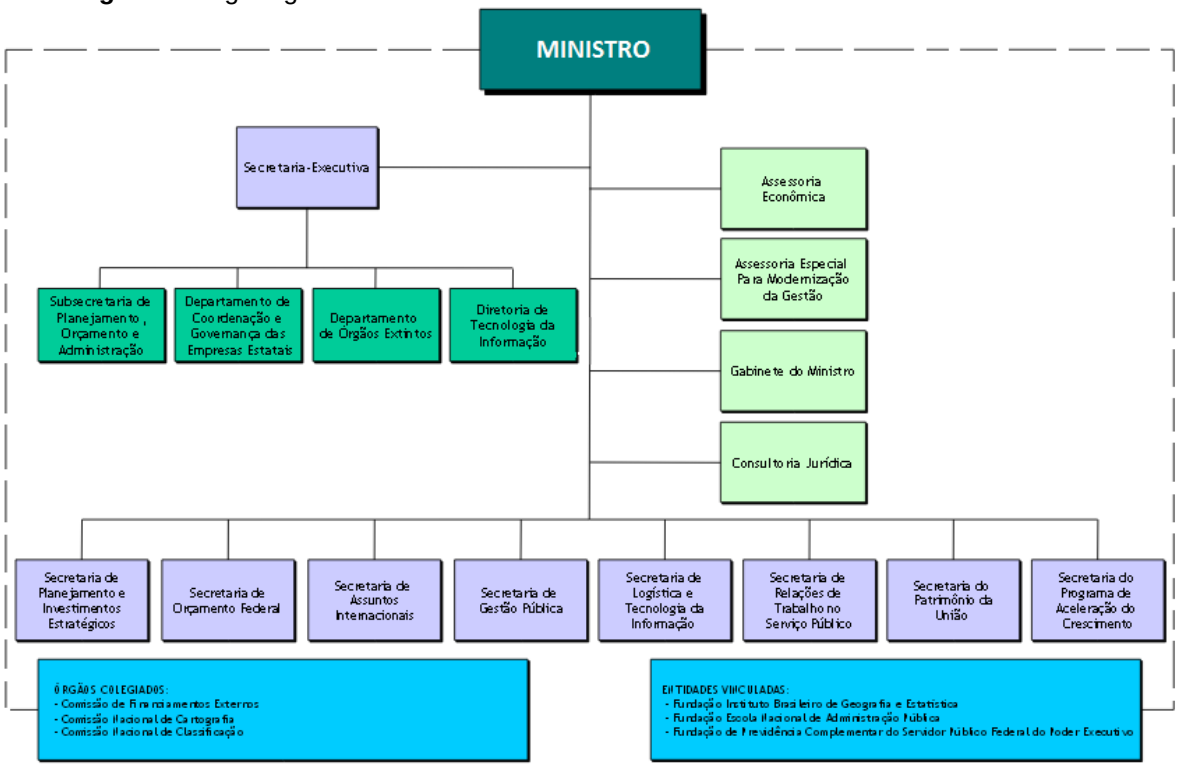
Figura 1: Organograma típico de ministérios



Fonte: Desenvolvido pelo autor em 2013.

Porém, esta é uma estrutura básica. 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, conforme foi representado pelas estruturas pontilhadas da figura 1. 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, três órgãos colegiados e três Fundações públicas diretamente vinculadas, e não subordinados, caracterizados na imagem por linhas pontilhadas.

Figura 2: Organograma diferenciado.



Fonte: http://www.planejamento.gov.br/ acesso em: 15 de Agosto de 2013

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, doravante SPOA. As SPOA's são supervisionadas pelas secretarias executivas e tem 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 (Decreto nº 6.061, 2007, Anexo I), no âmbito do Ministério a qual está vinculada.

Essas atribuições foram retiradas do documento de estrutura regimental do Ministério da Justiça, porém, podem ser vistas na maioria dos decretos de fundação dos Ministérios com atribuições idênticas ou muito similares.

1.1. O MINISTÉRIO DA JUSTIÇA

O Ministério da Justiça é o órgão superior da administração federal brasileira que trata das matérias relacionadas com a ordem jurídica, cidadania e garantias pessoais. A história do Ministério da Justiça remonta aos tempos do Brasil Império. Conforme um documento oficial do próprio Ministério da Justiça, a Cartilha para emendas orçamentárias de 2013:

> O Brasil possui Ministério da Justiça próprio desde o Decreto de 3 de julho de 1822, do Príncipe-Regente D. Pedro de Bragança, criando a Secretaria de Estado dos Negócios da Justiça. A Lei n. 23, de 30 de outubro de 1891, mudou a denominação para Ministério da Justiça e Negócios Interiores. Pelo Decreto-Lei n. 200, de 25 de fevereiro de 1967, passou a denominar-se simplesmente Ministério da Justiça.

O Ministério da Justiça teve sua estrutura regimental regulamentada e estabelecida conforme o Decreto nº 6.061, de 15 de março de 2007, Anexo I e alterações, com vigência a partir de 16 de Março de 2007.

O órgão tem por competência as seguintes atribuições:

> I - defesa da ordem jurídica, dos direitos políticos e das garantias constitucionais;
> II - política judiciária;
> III - direitos dos índios;
> IV - entorpecentes, segurança pública, Polícias Federal, Rodoviária Federal e Ferroviária Federal e do Distrito Federal;
> V - defesa da ordem econômica nacional e dos direitos do consumidor;
> VI - planejamento, coordenação e administração da política penitenciária nacional;
> VII - nacionalidade, imigração e estrangeiros;
> VIII - ouvidoria-geral dos índios e do consumidor;
> IX - ouvidoria das polícias federais;
> X - assistência jurídica, judicial e extrajudicial, integral e gratuita, aos necessitados, assim considerados em lei;

> XI - defesa dos bens e dos próprios da União e das entidades integrantes da administração pública federal indireta;
> XII - articulação, coordenação, supervisão, integração e proposição das ações do Governo e do Sistema Nacional de Políticas sobre Drogas nos aspectos relacionados com as atividades de prevenção, repressão ao tráfico ilícito e à produção não autorizada de drogas, bem como aquelas relacionadas com o tratamento, a recuperação e a reinserção social de usuários e dependentes e ao Plano Integrado de Enfrentamento ao Crack e outras Drogas; (Redação dada pelo Decreto nº 7.434, de 2011)
> XIII - coordenação e implementação dos trabalhos de consolidação dos atos normativos no âmbito do Poder Executivo; (Redação dada pelo Decreto nº 7.430, de 2011) (Vigência)
> XIV - prevenção e repressão à lavagem de dinheiro e cooperação jurídica internacional; e (Redação dada pelo Decreto nº 7.430, de 2011) (Vigência)
> XV - política nacional de arquivos. (Incluído pelo Decreto nº 7.430, de 2011) (Vigência)
> XVI - assistência ao Presidente da República em matérias não afetas a outro Ministério. (Incluído pelo Decreto nº 7.538, de 2011) (BRASIL, DECRETO Nº 6.061, DE 15 DE MARÇO DE 2007.)

O Ministério da justiça foi o primeiro ministério criado e possui uma estrutura robusta e pode ser considerado um órgão público de grande porte, com mais de 2000 colaboradores entre servidores, estáveis e comissionados, funcionários terceirizados, estagiários, além de consultores dos diversos projetos de cooperação técnica internacional de entidades como o Programa das Nações Unidas para o Desenvolvimento (PNUD) e Unesco, por exemplo. De acordo com dados presentes na sessão de recursos humanos do portal do Ministério da Justiça, considerando-se apenas a estrutura central do Ministério da Justiça e o Departamento Penitenciário Nacional (DEPEN), tem-se os seguintes números:

- Servidores : 1.212 (um mil, duzentos e doze)
- Terceirizados: 1.170 (um mil, cento e setenta)

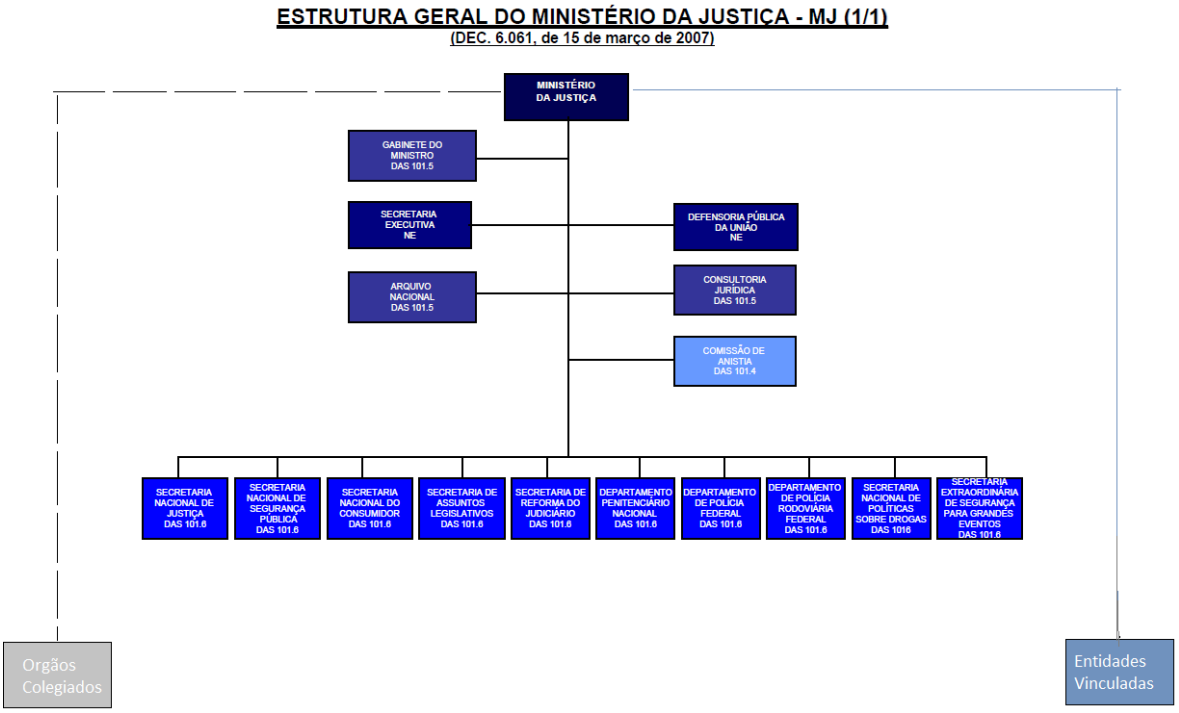
A soma desses dois segmentos totaliza 2.382 colaboradores apenas na estrutura central da organização e no DEPEN. O número de estagiários e

consultores não foi divulgado no portal, todavia, de acordo com uma matéria da revista ISTO É de 03/10/2013, estima-se que haja nove mil consultores em toda a esplanada dos ministérios. Assim, pode-se estimar que o número de colaboradores, dentre todos os vínculos mencionados, chegue aproximadamente ao número de 3.000 (três mil).

A maior parte de sua estrutura está no Palácio da Justiça e seus anexos, na esplanada dos ministérios em Brasília, porém, existem outras localidades importantes externas a esplanada, assim como as unidades estaduais de cada secretaria e as penitenciárias federais.

Abaixo o organograma do Ministério da Justiça:

Figura 3: Organograma do MJ



Fonte: Desenvolvido pelo autor em 2013.

Este organograma foi criado a partir do Decreto que instituiu o Ministério da Justiça, porém, poderá haver mudanças nessa estrutura com a criação de novas secretarias, departamento, dentre outros. Para efeitos desse artigo, será considerada a estrutura fundamental do órgão para a realização das 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.

Como de praxe, a estrutura segue o modelo clássico da maioria dos Ministérios com Consultoria Jurídica e Secretaria Executiva, subordinadas diretamente ao gabinete do Ministro. No caso do Ministério da justiça, a chefia do Gabinete do Ministro, a Secretaria Executiva, a Comissão de Anistia e a Consultoria Jurídica agem como órgãos de assistência direta e imediata ao Ministro de Estado. Já o Arquivo Nacional, a Defensoria Pública da União e os demais departamentos e secretarias dispostos na parte inferior do organograma são denominados como “órgãos específicos singulares”.

O Ministério da Justiça possui ainda seis órgãos colegiados, caracterizados pelas linhas pontilhadas e duas entidades vinculadas, caracterizadas pelas linhas de cor cinza, a saber:

Órgãos colegiados:

- Conselho Federal Gestor do Fundo de Defesa dos Direitos Difusos (CFDD);
- Conselho Nacional de Arquivos (CONARQ);
- Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual (CNCP);
- Conselho Nacional de Política Criminal e Penitenciária (CNPCP);
- Conselho Nacional de Políticas sobre Drogas (CONAD);
- Conselho Nacional de Segurança Pública (CONASP);

Entidades vinculadas:

- Autarquia: Conselho Administrativo de Defesa Econômica (CADE);
- Fundação: Fundação Nacional do Índio (Funai);

Para ampliar o entendimento dessa pesquisa, é importante abordar a atuação de algumas áreas específicas, como a Secretaria Executiva, a Subsecretaria de Planejamento, Orçamento e Administração (SPOA) e a Coordenação Geral de Tecnologia da Informação (CGTI).

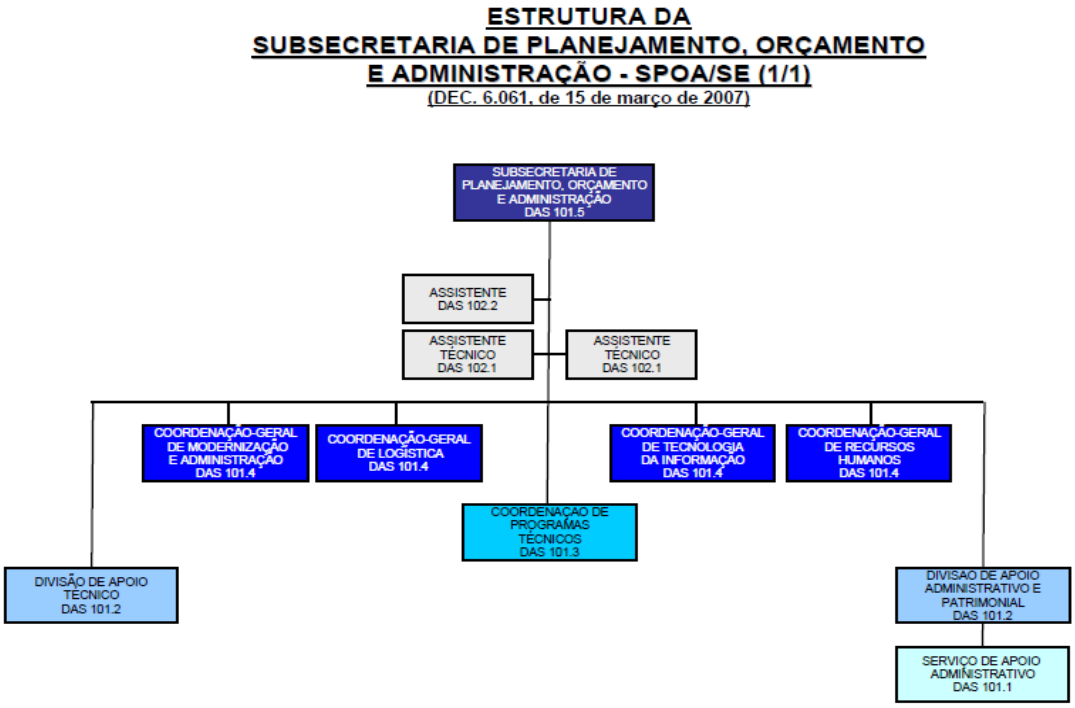
A Secretaria Executiva, além de todo apoio ao Gabinete na coordenação, supervisão e acompanhamento de programas e projetos ligados às estratégias do órgão, é a área diretamente ligada a Subsecretaria de Planejamento, Orçamento e Administração (SPOA). Esse setor será analisado com mais atenção, pois é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

Dentre outros, a SPOA tem por competência:

> I - planejar, coordenar e supervisionar a execução das atividades relativas à organização e modernização administrativa, assim como as relacionadas com os sistemas federais de planejamento e e de orçamento, de contabilidade e de **administração financeira, de administração de recursos de informação e informática, de recursos humanos** e de serviços gerais, no âmbito do Ministério;
> II - promover a articulação com os órgãos centrais dos sistemas federais, (...), e informar e orientar os órgãos do Ministério quanto ao cumprimento das normas administrativas estabelecidas; (BRASIL, arts. 5 do decreto no 6.061, de 15 de março de 2007) (grifos nossos)

Em sua composição, a SPOA tem as seguintes coordenações e divisões:

Figura 4: Organograma da SPOA



Fonte: <www.portal.mj.gov.br> acesso em 03/092013

A Coordenação Geral de Tecnologia da Informação é responsável pelo fornecimento de recursos de tecnologia da informação para todas as áreas da estrutura central do MJ. A maioria das secretarias citadas possui uma área independente de Tecnologia da Informação com desenvolvimento de sistemas e áreas de negócios de sistemas quase totalmente autônomas, tanto em termos de serviços prestados quanto de hardware.

É importante frisar a abrangência da prestação de serviços de TI que a estrutura central do MJ provê. Basicamente, quem consome diretamente, ou seja, serviços, hardwares, links de comunicação, telefonia e sistemas do MJ são:

- Estrutura central do MJ;
- SENASP;
- DEPEN;

- DRCI (SNJ);

O MJ abriga em sua estrutura sistemas que dão apoio aos seus projetos finalísticos e diretamente aos programas de governo que alcançaas grandes dimensões. São mais de 60 sistemas atualmente em ambiente de produção (dados do primeiro semestre de 2014). Vários sistemas que dão apoio a atividades como crimes de lavagem de dinheiro, segurança nacional, desaparecimento de pessoas, direitos humanos, direitos do consumidor, direito dos povos indígenas, leis antipirataria, combate ao tráfico, sistema de monitoramento de cidades, sistemas de controle carcerário, enfim, uma série de atividades que estão sob os refletores da imprensa e que tem grande visibilidade ao governo.

No bojo das áreas citadas, está o sistema INFOSEG que interliga uma rede nacional de agentes de segurança pública e no qual trafegam informações de alto grau de confidencialidade. Segundo o portal do Conselho Nacional de Justiça:

> A ferramenta interliga as bases federais e estaduais, consubstanciando-se em um Banco Nacional de Índices, que disponibiliza dados de inquéritos, processos, armas de fogo, veículos, condutores, mandados de prisão, entre outros, mantidos e administrados pelas Unidades da Federação e Órgãos Conveniados.
> A Infoseg consolida-se como o maior sistema de informações de segurança pública do país, buscando, em seu contínuo aperfeiçoamento, a integração e a interoperabilidade com os diversos sistemas e tecnologias no âmbito da segurança pública.

Recentemente houve uma série de matérias veiculadas na televisão brasileira com denúncias sobre a venda de senhas do INFOSEG por parte de agentes públicos, causando um verdadeiro escândalo televisivo, inclusive expondo os dados de pessoas públicas como o da presidente Dilma Roussef, o que abalou a credibilidade e imagem do Ministério da Justiça.

De acordo com a matéria veiculada no SBT no dia 11 de Março de 2013:

> “esquema de venda de senhas do INFOSEG, o maior banco de dados de Segurança Pública do país. A ferramenta possui informações de milhões de brasileiros, inclusive dos que já estão mortos, e é usada pela polícia para combater crimes. No entanto, em contato com um *cracker*, como é chamado um criminoso de internet, a equipe do jornal teve acesso a como é feita a violação do serviço.” (http://www.sbt.com.br/jornalismo/noticias/30510/Exclusivo:-SBT-Brasil-denuncia-venda-de-senhas-do-INFOSEG.html)

Com base no cenário exposto, pode-se perceber que as informações que trafegam no âmbito das redes, sistemas e bancos de dados do Ministério da Justiça exigem um alto grau de sigilo, não só por sua natureza, mas, por tratar informações de todos os cidadãos brasileiros.

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

1.2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO MINISTÉRIO DA JUSTIÇA

O Ministério da Justiça possui uma Política de Segurança da Informação e Comunicações, doravante POSIC, instituída por meio da portaria nº 3530 de 03/12/2013 / MJ, que versa sobre diretrizes gerais de segurança da informação para cumprimento de todos os colaboradores, órgãos e entidades do Ministério da Justiça. Essa portaria revoga a portaria nº 3.251, de 19 de dezembro de 2012, do Ministério da Justiça, a qual instituía a primeira política de segurança da informação da organização.

Este documento envolve a regulação de utilização de recursos de tecnologia da informação e comunicações como computadores, serviços de e-mail, internet, dentre outros.

De acordo com o artigo 1º da portaria nº 3530 de 03/12/2013, A POSIC do Ministério da Justiça tem como objetivo:

> dotar os órgãos e entidades da estrutura organizacional do Ministério de princípios, diretrizes, critérios e instrumentos aptos a assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações, protegendo-as contra ameaças e vulnerabilidades.

Dentre as diretrizes gerais, dispostas no artigo 4º da portaria em questão (op.cit,*idem*), vale destacar a seguinte diretriz: “elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de SIC em vigor”

A POSIC do MJ também prevê sanções administrativas como forma de penalidade para aqueles que descumprirem a política de segurança da informação e suas normas complementares.

Na seção I da POSIC (op.cit,*idem*) fica instituído o Gestor de Segurança da Informação e Comunicações, papel que deverá ser exercido por um servidor público efetivo designado pela Secretaria Executiva e cuja responsabilidades vão desde examinar, formular, promover e coordenar as ações de segurança da informação e comunicações no Ministério até a divulgação das políticas e normas complementares, solicitação de recursos, articulação com entidades externas de segurança da informação, acompanhamento de incidentes de segurança da informação e encaminhamento de casos omissos.

Finalmente, na Seção II, artigo 7º (op.cit,*idem*), fica instituído o Comitê Gestor de Segurança da Informação e Comunicações, formado por um representante, titular

e suplente, de vários órgãos ligados à estrutura do MJ, cujo as responsabilidades são:

> I - assessorar na implementação das ações de SIC no Ministério;
> II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;
> III - propor normas e procedimentos internos relativos à SIC, em conformidade com as legislações existentes sobre o tema;
> IV - auxiliar na elaboração dos planos de gestão de riscos e de continuidade e na definição das diretrizes de auditoria e conformidade no âmbito do Ministério;
> V - revisar a POSIC/MJ sempre que se fizer necessário;
> VI - elaborar relatórios periódicos de suas atividades, encaminhando-os ao Secretário-Executivo; e
> VII - indicar os integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

As reuniões do comitê são definidas para acontecimento a cada dois meses e suas deliberações do Comitê serão tomadas por maioria simples, presente a maioria absoluta de seus membros. A portaria trata o Comitê Gestor de Segurança da Informação como “serviço público relevante”, mas não há obrigatoriedade explícita em nenhuma parte.

CAPÍTULO 2

2. REFERENCIAL TEÓRICO

2.1. 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 80 com a publicação de artigos em periódicos específicos das cadeiras de administração como o *Administrative Science Quaterly, Organization Studies*, dentre outros (AKTOUF, 1994).

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 de teóricas, pode ser moldado e dinâmico, consonante com os objetivos, valores e 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 numa 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 isto 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.

Neste universo de discussões sobre a cultura organizacional há divergência de linhas de pensamento de autores sobre o tema. Existe uma corrente mais voltada para uma análise antropológica da cultura organizacional assim como, uma análise com um viés mais acadêmico voltado à administração. O artigo “Cultura organizacional em organização pública: as bases da mudança organizacional a partir da reforma gerencial”, trás uma abordagem detalhada sobre o tema e remete o seguinte questionamento: Se a cultura para Aktouf 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 desta 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).

Hofstede foi piscólogo da IBM, empresa global de computação. Nesta empresa ele teve a oportunidade de utilizar como universo de pesquisa os funcionários da empresa em mais de 50 países, obtendo 116.000 questionários respondidos. Ele denominou então o que seriam as chamadas “culturas nacionais”, diferenciando estatisticamente os países relativamente uns aos outros, a partir de uma mesma empresa. O autor chegou a algumas dimensões culturais bipolarizadas, em que alguns países apresentavam índices mais altos e outros mais baixos, caracterizando assim sua cultura de acordo com aqueles valores pré-definidos de sua pesquisa (BRASILEIRO, 2007).

Na perspectiva de Certo (2003), sete características básicas, 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 à atenção aos detalhes; busca por resultados, o quão a organização está empenhada em alcançar resultados ao invés de apenas como ela vai alcançar esses resultados, como por exemplo, pelos processos e procedimentos os 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 mantêm estáveis mesmo em processo de constante crescimento. (CERTO, 2003)

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. Esta análise não pode ser aplicada totalmente a organizações governamentais. Mesmo a cultura sendo formada por valores nacionais e sociais, a 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 A Lei 8112/90, 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, Guimarães (2000 *apud* Pires ; Macedo, 2006, 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 diversas 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 se tratando da parte estratégica. Isto implica também em uma provável, e quase certa mudança de direcionamento, seja por ideologia, interesses e diretrizes do novo governo.
- Órgãos do governo, em sua maioria, não buscam o 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 uma efetividade de alcance de um objetivo caso não haja interesses compatíveis.

Esses fatores caracterizam a empresas do governo e refletem a distância que as separa da cultura que é mais comum às corporações privadas. Conforme

Carbone (2000, p. 234), algumas características de organizações públicas do Brasil são:

> **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;
> **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)

2.2. A SEGURANÇA DA INFORMAÇÃO

A competitividade e o dinamismo do mundo contemporâneo fazem com que as empresas e os governos invistam a 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. Neste 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* (2008) 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, disponibilidade. Sobre isto, Moreira (2001, p.9) diz que “o objetivo da segurança, no que tange à informação, é a busca da disponibilidade, 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 à 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 este 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-á apenas o pilar confidencialidade, integridade e disponibilidade.

Estes 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) 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 consequências 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. (Grifos nossos)

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 onde qualquer sistema está susceptível a um ataque, é uma condição causada muitas vezes pela ausência ou falta de efetividade das medidas que visam salvaguardam 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 frequência os inúmeros acontecimentos que poderão ocorrer, este tipo de análise nos aponta os possíveis perigos e suas consequências 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, se perceber que em aspectos de segurança física a organização está bem posicionada, mas, em contrapartida, deixa muito a desejar no que tange a

segurança lógica de seus sistemas. Desta forma, pode-se avaliar a segurança da informação sob diferentes prismas, tais como: Segurança física e segurança lógica.

Neste 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 a 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, 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 já 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 esta 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 (incêndios, 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 outro 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 Negócio , doravante denominado PCN, entra em ação quando ocorrem situações extremas que causam grandes danos aos negócios. Este 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 paraquedas reserva em momento de falha principal, garantindo, apesar do susto, a vida do paraquedista em queda”.

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

Suponha que o INSS, quando ocorrido o fatídico incêndio em Brasília no ano de 2005 - em que uma série de processos foram completamente perdidos - tivesse um Plano de Continuidade de Negócios instituído. Certamente as atividades teriam sido interrompidas por menos tempo, haveriam muito menos processos destruídos, porque provavelmente haveria contingenciamento dos dados e o transtorno para a sociedade seria muito menor. Quando se fala nos atentados terroristas de 11 de Setembro nos Estados Unidos da América, um clássico exemplo do meio acadêmico, não há como mensurar quantas empresas foram à falência, ou 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 *datacenters* espelhados na segunda torre, por exemplo.

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 acima, vale destacar o Cobit da ISACA e a família de normas da ISO 27.000, incluindo a ISO 27.001 e a ISO 27.002.

O *Control Objectives for Information and related Technology* (COBIT), foi publicado pela ISACA em 1996. Está em sua 5ª (quinta) edição e seu desenvolvimento contou com a participação de especialistas de todo o mundo, considerando as melhores práticas, metodologias, padrões profissionais para controle interno e requerimentos legais de diversos segmentos de mercado que dependem de tecnologia (ISACA, 2010).

O Cobit fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável, mas sem definir o "como" se fazer, apenas propõe uma série de controles básicos que proporcionarão um alinhamento da tecnologia da informação com os objetivos de negócio. (PONTES, 2012).

Para Alves (2006, p.29) o Cobit:

> 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.

Sobre os objetivos do COBIT, o IGTI (2007) os define como:

- Estabelecer relacionamentos com os requisitos do negócio;
- Organizar as atividades de tecnologia da informação em um modelo de baseado em processos;
- Identificar os principais recursos de tecnologia da informação;

- Definir os objetivos de controle que serão considerados para a gestão.

Dessa forma, o COBIT configura-se como uma poderosa ferramenta para gestão e melhores práticas de tecnologia da informação, assim como, sugere meios de controle com fins de prover o alinhamento de TI com o negócio.

A norma ISO 27001:2005 é a evolução da norma 17799:2000 que, por consequência, é originária da norma britânica British Standard (BS)7799. Essas normas passaram por diversos estágios evolutivos até alcançarem o status atual. 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 num total de 27 controles. (SÊMOLA, 2003).

De acordo com Fernandes e Abreu (2008, p. 352):

> A ISO/IEC 27.001:2005 foi preparada para prover um modelo para estabelecer, implantar, operar, monitorar, rever, manter e melhorar um Sistema de Gestão da Segurança da Informação (“Information Security Management System – ISMS”). Esta norma internacional pode ser usada visando a avaliação da conformidade por partes interessadas internas e externas.

Fernandes e Abreu (2008) ainda citam como objetivos do Sistema de Gestão da Segurança da Informação (SGSI) os seguintes:

- Definição do escopo e dos limites do SGSI;
- Definir a política de SGSI;
- Definir a abordagem e realizar a avaliação de riscos da organização;

- Analisar, avaliar os riscos e identificar opções e os controles para o tratamento dos riscos;
- Obter aprovações da administração para implementar e operar o SGSI;
- Elaborar uma declaração de aplicabilidade envolvendo os objetivos, os controles em si e sua justificativa e quaisquer ações – incluindo a implantação, exclusão, motivos - dos controles existentes.

A ISO 27.002, por sua vez, é a norma estrutural de gestão de segurança da informação. Ela define um código de boas práticas para a gestão da segurança da informação e indica quais os elementos devem ser considerados para uma adequada proteção da informação. Este código de boas práticas reúne 133 controles de segurança, distribuídos em 39 objetivos de controles. Muitos destes controles são relacionados à Tecnologia da Informação, porém, há aqueles embasados na estrutura organizacional das corporações, envolvendo fatores como cultura. (PONTES, 2012)

Conforme a própria publicação da ISO 27002, a ABNT (2005), p. 1, define:

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessários, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos.

Os objetivos de controle e os controles desta norma têm como finalidade ser implantados para atender aos requisitos identificados por meio de análise/avaliação de riscos. Esta norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas

de gestão da segurança, e para ajudar a criar confiança nas atividades interorganizacionais. (ABNT, 2005).

Conforme Pontes (2012, p. 24), os controles desta norma são:

> os elementos que definem o que a norma considera importante para um processo de segurança da informação na organização e devem ser os elementos considerados para as políticas de segurança da informação das organizações.

Assim, uma norma complementa a outra, sendo que a ISO 27001 atua como um padrão de gestão baseados em requisitos de auditoria para implementação do Sistema Gerenciador de Segurança da Informação, enquanto a ISO 27002 fornece um guia de implementação baseados no conjunto de controles em melhores práticas para a segurança da Informação. Ela não deve ser utilizada em auditorias, mas simplesmente servir como um guia, trazendo resultados mais tangíveis e aplicáveis.

2.3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIC)

A segurança da informação envolve uma série de fatores que transcendem a tecnologia da informação e, para que tenha relevância dentro das organizações, é interessante que haja um documento que norteie os objetivos do conjunto de diretrizes e as responsabilidades relacionadas à segurança da informação para que atinja todos os níveis organizacionais.

Para Beal (2005, p.43) “(...) A Política de Segurança da Informação estabelece linhas-mestras a serem seguidas na implementação da segurança da informação, formalizando todos os aspectos relevantes para a proteção, o controle e o monitoramento de seus ativos de informação.”

O objetivo da política de segurança da informação é fornecer orientação e apoio às ações da gestão de segurança da informação sobre os requisitos de

negócios e as leis e regulamentos pertinentes. O alto escalão, ou seja, o nível estratégico da organização deve estabelecer uma política clara e de acordo com os objetivos do negócio e demonstrar seu comprometimento com a segurança da informação através da publicação e manutenção de uma política para toda a organização (ISO/IEC 27002:2005, p.12).

A fim de ressaltar a importância desse documento no contexto de segurança da informação em uma companhia, Poltier *apud* Pontes (2012, p. 17) afirma:

> O primeiro e mais importante aspecto da segurança da informação é a política de segurança. Se a segurança da informação fosse uma pessoa a política seria o sistema nervoso. Política é a base da segurança da informação, providencia a estrutura e define os objetivos dos demais aspectos de segurança da segurança da informação.

Dessa forma, esse conjunto de regras não surge de forma aleatória, mas têm como ponto de partida normas e metodologias de boas práticas em segurança da informação como a ISO/IEC 27001/27002, as demais normas da família 27000 e o COBIT, por exemplo.

Sobre esse conjunto de diretrizes, a norma ABNT NBR ISO/IEC 27002 (2005, p.8) algumas diretrizes devem ser seguidas, são elas:

- Uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita compartilhamento da informação;
- Uma declaração do comprometimento da direção, apoiando as metas e princípios de segurança da informação, alinhada com os objetivos e estratégias do negócio;
- Uma estrutura pra estabelecer objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;
- Breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo: 1) Conformidade com a legislação e com requisitos regulamentares e contratuais. 2) Requisitos de conscientização, treinamento e educação em segurança da informação; 3) Gestão da continuidade de negócio consequência das violações na política de segurança da informação; 4)Definição

> das responsabilidades gerais e específicas na gestão de segurança da informação, incluindo os registros dos incidentes de segurança da informação; 5) Referências a documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mas detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

Uma vez definidas, as diretrizes devem partir do mais alto nível hierárquico da empresa, numa abordagem *top down*, ou seja, de cima para baixo a fim de comprometer e se fazer cumprir as definições da política de segurança da informação em todos os níveis organizacionais.

De acordo com Sêmola (2003, p. 105) a política de segurança deve ser: “(...) subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégica, tática e operacional”.

Assim, entende-se que a política de segurança da informação vai dar direção aos objetivos de segurança da informação da organização e poderá ser apoiado por documentações complementares que irão se aprofundar em controles específicos.

2.4. 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 ou decretos ou por regulações do próprio mercado que clamam por conformidade na adoção de procedimentos de segurança. Esses procedimentos muitas vezes estão inclusos numa série de premissas envoltas em um contexto de Governança Corporativa. Governança é diferente de Governar: a Governança Corporativa tem muito haver com prestação de contas, transparência e responsabilidade corporativa, enquanto governar é se 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 passaram a vigorar, a exemplo da lei americana *Sarbanes Oxley*, doravante 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) 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, fuga de investidores, claramente causada por desconfiança ou descredibilidade da empresa perante o mercado, há uma referência direta à aspectos de segurança da informação. Dentro deste 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.

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

Constituição Federal existem diversos aspectos ligados à segurança das informações, direta ou indiretamente. O artigo 5º, inciso XXXIII e art. 37, § 3º, inciso II, por exemplo, tem 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. Nos artigos 23, incisos III e IV e artigo 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, no ano 2000, o decreto 3.505 de 13 de Junho, da Presidência da República, instituía a Política de Segurança da Informação nos órgãos e entidade da Administração Pública Federal. Este 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, trata-se de obrigatoriedade e de conformidade. Certamente, o decreto fala também de conscientização, programas de capacitação, divulgação e até a instituição de um comitê para auxiliar os demais órgãos a alcançarem este objetivo.

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

> (...)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, Decreto nº 3.505, 2000.) (grifos nossos)

O artigo 6º da lei 10.683 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, Lei No 10.683, de 28 de Maio de 2003).

O Decreto número 7.845, de 14 de novembro de 2012, regulamenta procedimentos para o credenciamento de segurança e tratamento de informação

classificada em qualquer grau de sigilo no âmbito do Poder Executivo federal, e dispõe sobre o Núcleo de Segurança e Credenciamento. Desta forma, fica clara a responsabilidade do agente público pelo manuseio de informações no âmbito da administração pública e a necessidade de classificação e manuseio da informação.

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

Complementarmente, 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 B 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.

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

CAPÍTULO 3

3. ANÁLISE E RESULTADOS

Conforme descrito no capítulo da Metodologia Científica, os próximos dois subitens estarão dedicados à aplicação dos métodos de pesquisa.

3.1. ANÁLISE DOS FATORE ESTRUTURAIS

Percebe-se grande dificuldade na implantação de políticas que implicam em aspectos culturais 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.

Nesse contexto faz-se necessário conectar o organograma ao cenário político, o qual é estreitamente ligado à ocupação de posições nesse organograma e na continuidade de programa e políticas públicas e consequentemente, políticas internas também.

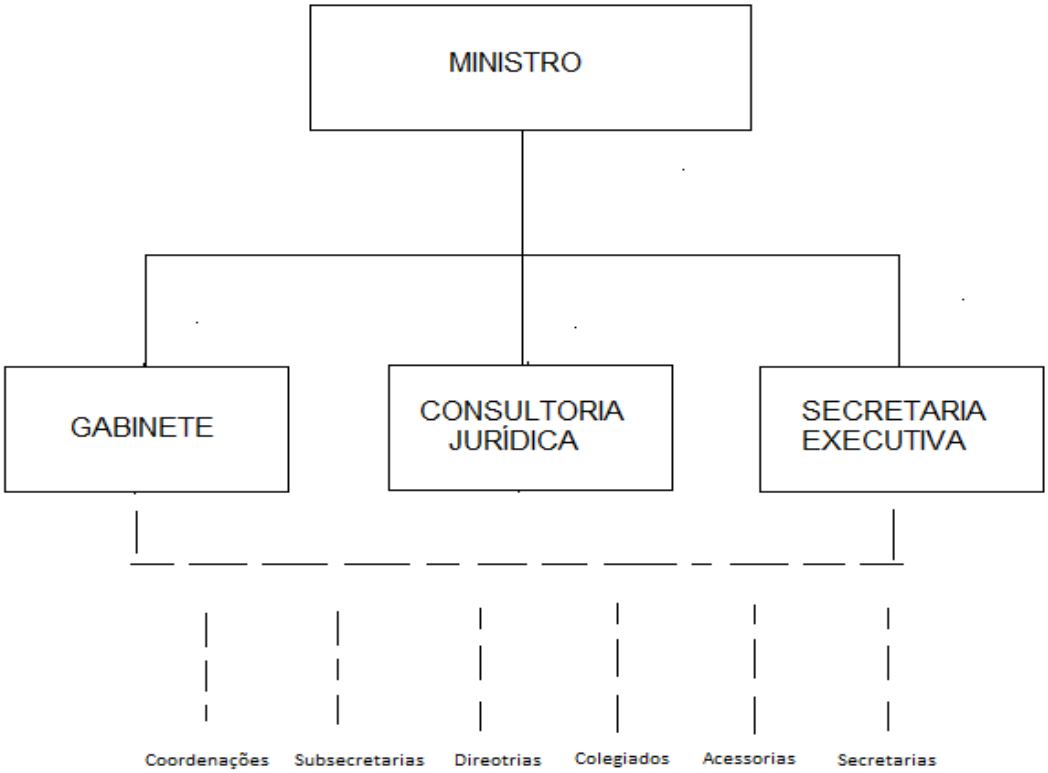
Os organogramas estão presentes na maioria das empresas e representam, de forma visual, os fluxos de autoridade, as responsabilidades departamentais e suas funções, geralmente numa abordagem do topo para a base (KWASNICKA, 2007).

Sobre organogramas, Daychouw (2007, p. 188) afirma que:

> Em um organograma os órgãos são dispostos em níveis que representam a hierarquia existente entre eles. Em um organograma vertical, quanto mais alto estiver o órgão, maior a autoridade e a abrangência da atividade.

Conforme foi demonstrado no capítulo 2 “Os Ministérios”, o organograma das organizações da Administração Pública Federal tendem a ter uma estrutura similar, vertical e que geralmente obedecem à estrutura:

Figura 5: Organograma típico



Fonte: Desenvolvido pelo autor em 2013.

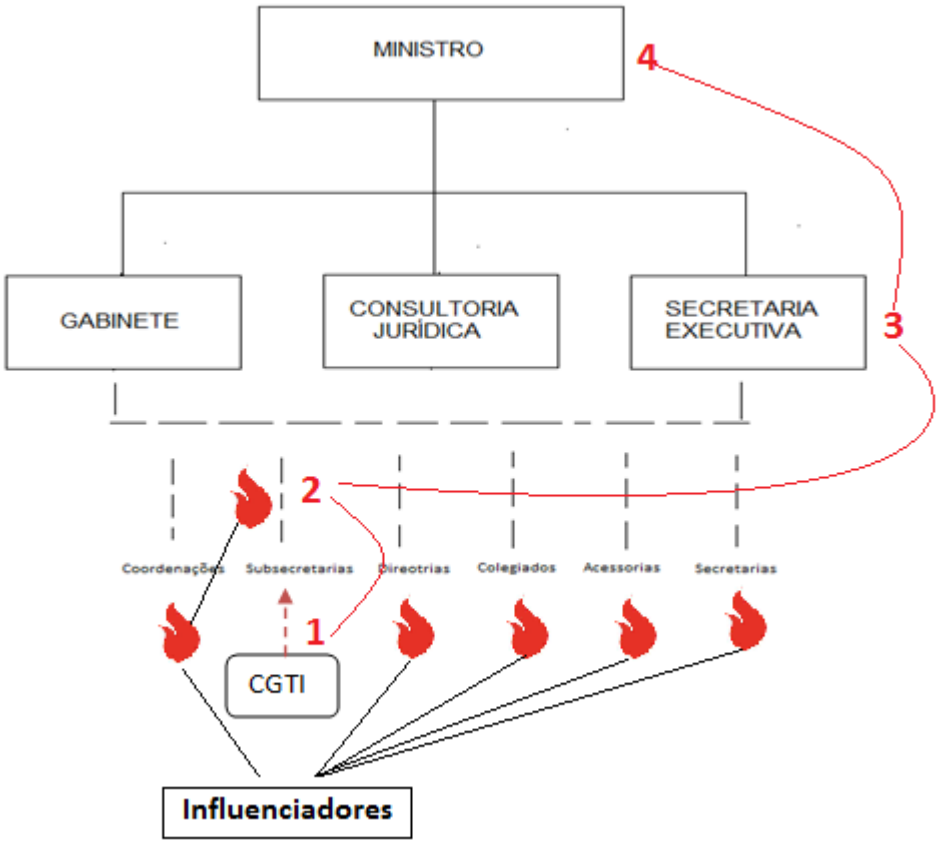
Partindo para uma análise do organograma do Ministério da Justiça, pode-se perceber alguns fatos que colocam a implantação da política de segurança da informação em desvantagem em termos de aplicação de controles e mudança de paradigmas em larga escala no Ministério da Justiça:

- O órgão não dispõe em seu organograma nenhuma referência a uma área de segurança da informação. Existe uma área de segurança corporativa ligada ao gabinete do Ministro, porém, nenhuma referência é

feita com relação a Segurança da Informação, tampouco na área de Tecnologia da Informação – CGTI;

- Para a aprovação de um novo controle ou para fazer valer as campanhas de apoio a divulgação e programas de educação voltados a Segurança da Informação com o objetivo de cumprir com as diretrizes definidas na Política de Segurança da Informação, seriam necessários pelo menos 4 (quatro) saltos hierárquicos para que uma medida expedida pela área de Tecnologia da Informação chegasse ao Ministro, observe a figura abaixo:

Figura 6: Fluxo de autoridade MJ



Fonte: Desenvolvido pelo autor em 2013.

Algumas das vantagens da utilização de organogramas em uma empresa são: auxiliar a graduar e classificar trabalhos e tarefas e permitir visualização maior

das necessidades de mudanças organizacionais e de crescimento da empresa. Em contra partida, como um ponto negativo dessa abordagem estrutural, é que ele demonstra apenas uma dimensão dos muitos tipos de relação que existem entre departamentos, não sendo fiel ao que ocorre no cotidiano das empresas. (KWASNICKA, 2007).

Assim, fica claro que é de extrema dificuldade alcançar os objetivos estabelecidos em uma Política de Segurança da Informação, mesmo que ela tenha sido aprovada formalmente pelo alto escalão da organização uma vez que os controles que devem ser posteriormente propostos irão esbarrar na aprovação ou boicote de diversas áreas com poder hierárquico e estratégico maior do que aquela área que gera essas medidas e controles.

Outro ponto que vale ser analisado é a sustentabilidade ou continuidade de planos ou políticas no âmbito do governo, uma vez que a rotatividade em cargos estratégicos é relativamente alta. De forma a exemplificar, de acordo com dados extraídos do Diário Oficial da União, entre 2011 e 2014 o cargo de Coordenador Geral de Tecnologia da Informação, vinculo maior entre as áreas de Tecnologia da Informação e a SPOA, foi alterado 3 (três) vezes. 1

[1] SECRETARIA EXECUTIVA PORTARIAS DE 7 DE JUNHO DE 2011- O SECRETÁRIO EXECUTIVO DO MINISTÉRIO DA JUSTIÇA, no uso da competência atribuída pelo inciso III, do art. 3º, da Portaria Ministerial nº 145, de 26 de janeiro de 2004, resolve:
Nº 1.033 - Exonerar, a pedido, JORILSON DA SILVA RODRIGUES do cargo de Coordenador-Geral de Tecnologia da Informação da Subsecretaria de Planejamento, Orçamento e Administração da Secretaria Executiva, código DAS 101.4.

SECRETARIA EXECUTIVA PORTARIAS DE 7 DE JULHO DE 2011- O SECRETÁRIO EXECUTIVO DO MINISTÉRIO DA JUSTIÇA, no uso da competência atribuída pelo inciso III, do art. 3º, da Portaria Ministerial nº 145, de 26 de janeiro de 2004, resolve:
N 1.297 - Nomear ALEXANDRE CARDOSO DE BARROS para exercer o cargo de Coordenador-Geral de Tecnologia da Informação da Subsecretaria de Planejamento, Orçamento e Administração da Secretaria Executiva, código DAS 101.4.

SECRETARIA EXECUTIVA PORTARIAS DE 23 DE MAIO DE 2014- O SECRETÁRIO EXECUTIVO DO MINISTÉRIO DA JUSTIÇA, SUBSTITUTO, no uso da competência atribuída pelo inciso III, do art. 3º, da Portaria Ministerial nº 145, de 26 de janeiro de 2004, resolve:

De acordo com Nogueira (2006, p. 13), em sua dissertação de mestrado sobre continuidade e descontinuidade administrativa em governos locais:

> Se não é possível afirmar que a questão da continuidade e da descontinuidade administrativa compõe um campo de estudos a ser desbravado, ainda assim chama à atenção a pequena quantidade de pesquisas realizadas sobre um assunto que figura como tese ou "lei" do dia-a-dia político brasileiro. No discurso presente no cotidiano de ministérios, fundações, secretarias, autarquias e empresas públicas, e por vezes reforçada pela imprensa, quando há troca de governo, a descontinuidade administrativa é dada como fato. Isso se traduziria na interrupção de iniciativas, projetos, programas e obras, mudanças radicais de prioridades e engavetamento de planos futuros, sempre em função de um viés político, desprezando-se considerações sobre possíveis qualidades ou méritos que tenham as ações descontinuadas. **Como consequência, tem-se o desperdício de recursos públicos, a perda de memória e saber institucional, o desânimo das equipes envolvidas e um aumento da tensão e da animosidade entre técnicos estáveis e gestores que vêm e vão ao sabor das eleições.** (grifos nossos)

Assim, a descontinuidade de políticas e ações internas, somadas à complexa estrutura organizacional e à cultural da organização vão se tornar fatores determinantes na implantação efetiva, ou não, da política de segurança da informação em uma organização pública.

De forma a enriquecer a análise, foi analisado o Plano Diretor de Tecnologia da Informação (PDTI) do Ministério da Justiça a fim de extrair dados referentes aos objetivos estratégicos da organização entre os anos de 2013 e 2015. A Instrução Normativa SLTI/MP nº 04/2008, de 19 de maio de 2008, posteriormente atualizada pela IN SLTI/MP nº 04/2010 determina a obrigatoriedade de elaboração de um Plano Diretor de Tecnologia da Informação para órgãos públicos. A Instrução Normativa SLTI/MP nº 04/2008 determina:

Nº 487 - Nomear MARCELO NOGUEIRA LINO para exercer o cargo de Coordenador-Geral de Tecnologia da Informação da Subsecretaria de Planejamento, Orçamento e Administração da Secretaria Executiva, código DAS 101.4.

> [...] Art. 3 item X - Plano Diretor de Tecnologia da Informação - PDTI: instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que visa atenda às necessidades de informação de um órgão ou entidade para um determinado período.

Dessa forma, o PDTI, documento público e de livre consulta, é um rico documento para exploração no que tange às necessidades de Tecnologia da Informação e as diretrizes que a organização pretende seguir a fim de alcançar as metas planejadas. Nesse documento, é possível verificar uma matriz SWOT (*strenghs, weaknesses, opportunities and threats*)2

Ao analisar a matriz SWOT do PDTI 2013/2015 do Ministério da Justiça (2013, P 41), na parte de ameaças, tem-se o seguinte:

> a) Número de concursos insuficientes para suprir a carência de servidores na área de governança de TI da APF; b) Número de concursos insuficientes para suprir a carência de servidores na área técnica de TI da APF; c) Corte de orçamento; **d) Interferência política externa que impacta nas decisões estratégicas e operacionais internas;** e) Percepção negativa dos usuários da qualidade dos serviços prestados;**f) Falta de recursos físicos e financeiros para os projetos estratégicos de TI; g) Falta de apoio aos projetos estratégicos de TI; h) Estrutura organizacional insuficiente e inadequada da área de TI; i) Posicionamento inadequado na estrutura organizacional com base no acórdão nº 1163/2008 - TCU;** j) Inexistência de Planejamento Estratégico do órgão institucionalizado; **k) Área de TI tratada como área meio e não estratégica;** l) Quantitativo inadequado de servidores; m) Elevado volume de contratos geridos e fiscalizados por número inadequado de servidores;(grifos nossos)

O que fica claro é que, a análise do organograma realizada por um agente externo, o autor, por si só já diagnostica dificuldades no fluxo de aplicação de políticas e boas práticas. Complementarmente, a visão dos colaboradores do órgão

[2] Trata-se de uma metodologia para análise de forças, fraquezas, oportunidades e fraquezas (em português). A Análise SWOT é uma ferramenta utilizada para fazer análise de cenário de ambiente, sendo usada como base para gestão e planejamento estratégico de uma corporação ou empresa, mas podendo, devido a sua simplicidade, ser utilizada para qualquer tipo de análise de cenário (http://pt.wikipedia.org/wiki/Análise_SWOT)

corrobora com esse cenário, principalmente pela clareza com a qual as ameaças são expostas, destacadas em negrito. Em relação ao item “D”, o problema estrutural fica claro quando os cargos de escalões mais altos do Ministério são provenientes de indicações político-partidárias e que ocupam cargos de decisão e estão hierarquicamente acima da área onde os controles para boas práticas de segurança da informação são elaboradas. Perceba que, caso uma diretriz seja definida e tenha que ser seguida por toda a organização, não há força para que ela seja amplamente cumprida caso pessoas com grande influência não as queiram seguir, causando um efeito cascata com os níveis abaixo dessa função.

O item “G” indica o não cumprimento de uma das principais premissas para a implantação bem sucedida de uma política de segurança da informação, conforme sugere o padrão de boas práticas em segurança da informação como a ISO 27001 (2006, pag. 4), a saber:

> A Alta Direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios: a) assegurando que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização; b) garantindo a integração dos requisitos do sistema de gestão de segurança da informação dentro dos processos da organização; c) assegurando que os recursos necessários para o sistema de gestão de segurança da informação estejam disponíveis; d) comunicando a importância de uma gestão eficaz de segurança da informação e da conformidade com os requisitos do sistema de gestão de segurança da informação; e) assegurando que o sistema de gestão de segurança da informação alcança seus resultados pretendidos; f) orientando e apoiando pessoas que contribuam para a eficácia do sistema de gestão de segurança da informação; g) promovendo melhoria contínua; e h) apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica á áreas sob sua responsabilidade.

O item “F”, falta de recursos físicos e financeiros para os projetos estratégicos de TI, torna-se então um problema igualmente estrutural por se tratar de

dependência de liberação de recursos e projetos que dependem de níveis hierarquicamente superiores e que, se descomprometidos, impactam diretamente na implantação de controles e da política. Os itens “H” e “I”, dizem respeito diretamente a problemas estruturais: “estrutura organizacional insuficiente e inadequada da área de TI” e “posicionamento inadequado na estrutura organizacional com base no acórdão nº 1163/2008 – TCU”. Em relação ao primeiro item (H) não fica claro o que é a “estrutura organizacional insuficiente”, porém, o tópico sugere insatisfação com a forma atual da estrutura, o que já dá base para um olhar cuidadoso sobre essa questão.

O item “I” referencia um acórdão do TCU que se trata de auditoria realizada na Secretaria Executiva do Ministério da Justiça, entre os dias 9/10 e 7/12/2007, visando avaliar a terceirização no setor de Tecnologia da Informação - TI de entes da Administração Pública Federal, em especial no que concerne à adequação da estrutura da unidade e aos processos de aquisição e gestão de serviços terceirizados. Sobre esse documento, vale ressaltar alguns pontos que colaboram com o objeto dessa pesquisa:

No subitem 8.3 Setor de TI - comitês estratégicos e de direção de TI – (*op.cit., idem*) inexistência/falhas, tem-se o seguinte:

> - b) por meio de entrevista, foi constatada ainda a existência do Comitê Gestor de Segurança da Informação (SI);
> - c) (...) embora contem com representantes das diversas áreas do MJ, tratam de assuntos específicos (infovia e segurança da informação). Não existe um comitê com autoridade e poderes decisórios para deliberar sobre investimentos na área de TI como um todo (tecnologia, aplicativos, projetos, sistemas, hardware, software, pessoal, infraestrutura e microcomputadores). **A falta de uma instância superior para definir as prioridades do setor de TI gera disputa interna entre os gestores do Ministério desejosos de primazia nos trabalhos que gerenciam.**
> - d) **essa falha pode ocasionar a não implementação de projetos** e a incerteza por parte do ordenador de despesa com relação às reais necessidades das solicitações de compras por parte da

> CGTI. Ademais, não existem critérios para o processo decisório que determina a priorização e execução das ações e investimentos em TI; (grifos nossos)

No subitem 8.4, Setor de TI - posicionamento inadequado (op.cit., idem), o diagnóstico do TCU enumera de forma definitiva possíveis fatores estruturais e dificultadores para a implantação de políticas no âmbito do Ministério da Justiça, que pode se aplicar perfeitamente para a política de segurança da informação, a saber:

> - a) por meio do subitem 3.2 do Anexo I ao Ofício nº 748/2007-Secex-6 (fls. 2 e 13 do vol. principal), foi solicitado o organograma da Coordenação-Geral de Tecnologia da Informação (CGTI), o qual foi encaminhado à equipe de auditoria;
> - b) a CGTI está subordinada a um dos departamentos de usuários (Subsecretaria de Planejamento, Orçamento e Administração) **e está situada no quarto escalão do Ministério. Por ser considerada estratégica, a área de TI deveria estar localizada na estrutura organizacional de forma independente dos departamentos de usuários e a uma proximidade adequada da alta administração, de modo a possibilitar o estabelecimento de uma parceria entre eles**;
> - c) **por estar localizada hierarquicamente em posição de igualdade com os setores usuários da área de TI, a CGTI tem dificuldades para implementar procedimentos referentes à TI (Normas Internas, procedimentos para aquisições e terceirizações, políticas de TI, entre outros) que permeiam todo o Ministério (...)**
> - d) **o posicionamento inadequado do setor de TI acarreta dificuldades para a execução de atividades que permeiam todo o Ministério e a implementação de políticas e normas atinentes à TI que sejam obrigatórias para todo o Ministério;**
> - e) **a CGTI não se apresenta em posição estratégica no organograma do MJ, privando-se de autonomia necessária para atuar adequadamente no suporte aos objetivos finalísticos do Órgão.**
> - f) propõe-se recomendar à Secretaria Executiva do Ministério da Justiça que avalie a possibilidade de posicionar hierarquicamente a Coordenação-Geral de Tecnologia da Informação de modo independente dos setores usuários para facilitar sua atuação e a implementação de políticas de TI no âmbito do Ministério(...) (grifos nossos)

Por último, o parágrafo acima, do subitem 8.4, também torna a ameaça ”K” do PDTI, área de TI tratada como área meio e não estratégica, como um problema estrutural pelo fato da área de tecnologia da informação, da qual deriva

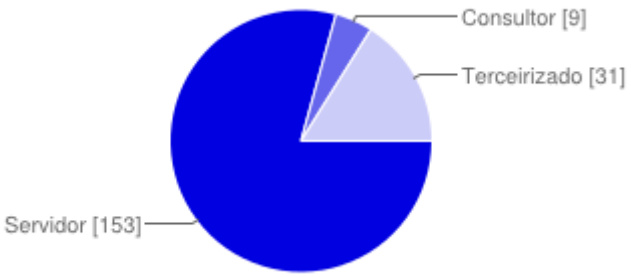
procedimentos, controles e normativos, não ter acesso ao alto escalão da organização e logo, não ter influenciadora em suas ações.

Mesmo tratando-se de uma auditoria realizada em 2007, parece que não houve muitos avanços em relação aos itens específicos já que figuram como ameaças pendentes de tratamento no Plano Diretor de Tecnologia da Informação 2013/2015. Salvo como exceção a criação do comitê de segurança da informação do Ministério da Justiça instituído junto à portaria nº 3.530, de 3 de Dezembro de 2013, a qual também institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça.

3.2. ANÁLISE DE PERCEPÇÃO E CULTURA ORGANIZACIONAL

1- Por favor, informe seu vínculo com o MJ:

Figura 7: Vínculo



Servidor	153	79%
Consultor	9	5%
Terceirizado	31	16%

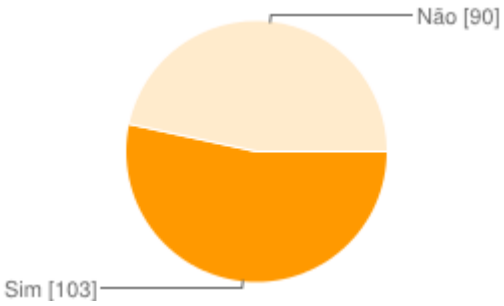
Fonte: Desenvolvido pelo autor em 2013.

Do universo total de entrevistados, um total de 79% foi composto por servidores do quadro do Ministério da Justiça, um total de 5% de consultores e 16% de terceirizados. Observando esses dados e pelo grande número de servidores, pode-se inferir que esse comportamento se dê pelo senso de propriedade pelos assuntos do órgão e estabilidade característica do funcionalismo público. Como as

duas outras categorias têm vínculos passageiros com a administração pública, é natural que o número de respostas seja menor. É importante ressaltar que, por mais que uma política de segurança da informação deva abranger a todos, é salutar que as chefias, gerencias departamentais e formadores de opinião dentro de uma organização estejam alinhados e em conformidade com os objetivos da política e suas boas práticas. Como em órgãos públicos todas - ou a maioria – das chefias são formadas por servidores, esse percentual não figura de forma negativa, apesar de não abranger grande parte dos terceirizados que são, em termos de números, quase iguais a servidores e possuem acesso a documentos, sistemas e a dependências da organização.

2- Você tem conhecimento de algum normativo/recomendações do MJ voltados à informática?

Figura 8: Normativos MJ



Sim	103	53%
Não	90	47%

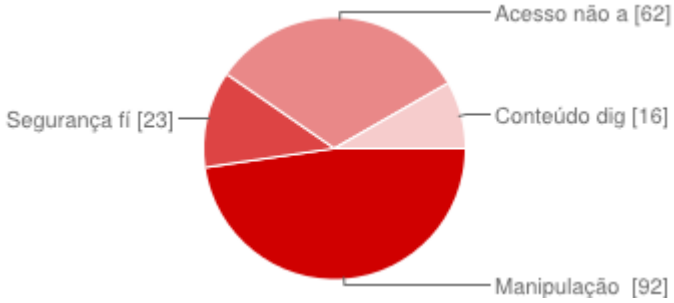
Fonte: Desenvolvido pelo autor em 2013.

Normativos são preceitos, muitas vezes arbitrários, que estão dispostos sobre forma de documentos e que versam sobre procedimentos e boas práticas dentro de uma organização. Uma política de viagens e reembolsos, política de uso de senhas, política de uso de sistemas corporativos e a própria política de segurança da informação são normativos organizacionais que todo colaborador deveria seguir. Em relação a essa questão, um total de 53% dos entrevistados respondeu conhecer

normativos do Ministério da Justiça relacionados à informática. Os outros 47% disseram desconhecer do assunto, o que corresponde a aproximadamente a metade dos entrevistados. Isso representa um desconhecimento considerável em relação ao que o órgão espera de seus colaboradores em relação ao uso de recursos computacionais, o que envolve, dentre outros: uso de senha, uso de informações de sistemas corporativos, uso da internet e e-mails, uso de recursos computacionais, uso de softwares e equipamentos pessoais, responsabilidades, direitos e deveres enquanto funcionário.

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

Figura 9: Elementos segurança da informação.



Fonte: Desenvolvido pelo autor em 2013.

Manipulação de informações sigilosas	92	48%
Segurança física do ambiente de trabalho	23	12%
Acesso não autorizado de pessoas à ambientes do MJ	62	32%
Conteúdo digital sobre o MJ	16	8%

O objetivo primordial dessa questão foi mensurar o que os colaboradores julgam importante quando se trata de segurança em seu ambiente de trabalho, dentro das opções propostas sendo que duas se referiam a questões físicas – segurança física no ambiente de trabalho e acesso não autorizado de pessoas ao ambiente do Ministério da Justiça – e duas que se referiam a questões lógicas – manipulação de informações sigilosas e conteúdo digital sobre o MJ. Apesar de

manipulação de informações sigilosas não se restringir apenas ao meio digital, muitos processos físicos, documentos, memorandos, pareceres e ofícios são armazenados em meio digital e trocados via correio eletrônico centenas de vezes durante o dia.

Assim, as respostas para essa questão ficaram divididas, sendo que 48%, que corresponde praticamente à metade dos respondentes, disseram se importar com a manipulação de informações sigilosas. De acordo com o relatório estatístico publicado pelo Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal – CTIR Gov, que apresenta algumas considerações sobre o trabalho de detecção, análise e resposta a incidentes de rede no âmbito do governo federal com referência ao período de abril a junho de 2014 em comparação com o 1º trimestre de 2014, incidentes de vazamento de informação passaram de 26 casos no 1º trimestre de 2014 para 243 casos no 2º Trimestre de 2014. (CTIR, 2014) Complementarmente, pode-se constatar que, historicamente, o governo brasileiro tem um largo histórico de vazamento de informações sigilosas, como por exemplo, o vazamento de provas do Exame Nacional do Ensino Médio (Enem), dados de processos de julgamentos políticos, divulgação de dados sensíveis de licitações, fraudes do INSS, dentre muitos outros fatos que sempre são amplamente divulgados na mídia e que podem justificar o grande percentual de respostas para esse item, até pelos recentes escândalos envolvendo o Ministério da Justiça em que senhas do sistema nacional de segurança pública Infoseg foram supostamente vendidas.

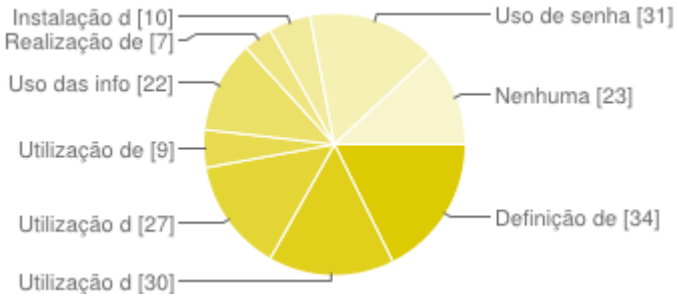
Por outro lado, 32% dos entrevistados reponderam que consideram o acesso de pessoas não autorizadas ao Ministério da Justiça o tópico mais importante em relação a segurança institucional. Esse percentual pode revelar dois vieses: o

primeiro é a preocupação com a integridade físicas das pessoas e o segundo é o acesso de estranhos a áreas restritas e logo, a informações restritas. A natureza do Ministério da Justiça é por si só de extrema sensibilidade, uma vez que manipula dados dos cidadãos, de processos, de fraudes, de criminosos, de leis, de direitos humanos, direito do consumidor e lavagem de dinheiro, por exemplo. Pessoas que manipulam essas informações certamente clamam por segurança física no trabalho, uma vez que a organização passa a ser alvo de ações maliciosas.

De forma similar 12% responderam que segurança física no ambiente de trabalho é o mais importante em termos de segurança institucional corroborando o item anterior (acesso de pessoas não autorizadas ao ambiente do órgão) e apenas 8% consideraram o conteúdo digital em relação ao Ministério da Justiça como importante em termos de segurança institucional, o que pode demonstrar pouca consciência sobre aspectos relacionados à segurança da informação numa perspectiva de segurança lógica, uma vez que 48% consideraram o mais preocupante a manipulação de informações sigilosas, mas que podem ser veiculadas em meio digital e que normalmente o são. Basta imaginar uma matéria contendo senhas e usuários de sistemas corporativos do Ministério da Justiça sendo divulgada na rede mundial de computadores: para além do prejuízo de imagem e credibilidade social da organização, a possível divulgação de uma informação como essa põe em risco a integridade dos colaboradores e do trabalho desses colaboradores. O item pode ser expandido para todas as frentes de trabalho do Ministério já citadas anteriormente.

4 - Dos itens a seguir, sobre qual você tem um maior conhecimento sobre procedimentos de segurança da informação?

Figura 10: Procedimentos segurança da informação.



Fonte: Desenvolvido pelo autor em 2013.

Definição de acesso a sistemas	34	18%
Utilização de e mail	30	16%
Utilização da internet	27	14%
Utilização de computadores	9	5%
Uso das informações institucionais	22	11%
Realização de Backup's	7	4%
Instalação de software's	10	5%
Uso de senhas	31	16%
Nenhuma	23	12%

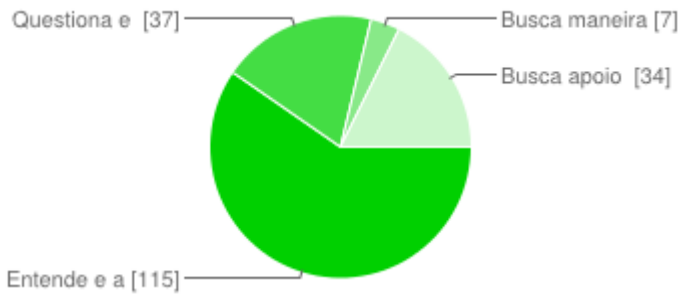
Com o objetivo de mensurar a familiaridade dos colaboradores em relação a procedimentos de segurança da informação em utilitários, facilidades e tecnologias utilizadas no dia a dia, essa questão revelou opiniões bem divididas sobre os tópicos apresentados. Os itens definição de acesso a sistemas, utilização de e-mails, utilização da internet e uso de senhas figuraram como os mais escolhidos, tendo como percentual 18%, 16%, 14% e 16% respectivamente. Ao analisar esses percentuais, percebe-se que são itens que se relacionam por se tratarem principalmente de softwares que são amplamente utilizados no cotidiano. Assim, é

natural que figurem mais do que itens como realização de backups, com 4% de respostas, instalação de softwares, com 5% de respostas e utilização de computadores, que são serviços geralmente entregues aos usuários, que possuem pouca ou nenhuma gerência sobre o assunto, tornando-os abstratos e transparentes. O item utilização das informações institucionais figura com um percentual significativo de respostas em detrimento do total de respostas, com 11%, e demonstra que uma parcela dos respondentes tem algum cuidado no que tange o uso de informações institucionais.

Um total de 12% afirmou não conhecer nenhum procedimento de segurança da informação em relação aos itens sugeridos, o que também representa uma parcela significativa do total de entrevistados e demonstra uma possível vulnerabilidade organizacional, uma vez que foram sugeridos itens genéricos sobre facilidades utilizadas diariamente por todos os colaboradores que responderam a pesquisa.

5 - 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:

Figura 11: Reação a bloqueios da segurança da informação.



Fonte: Desenvolvido pelo autor em 2013

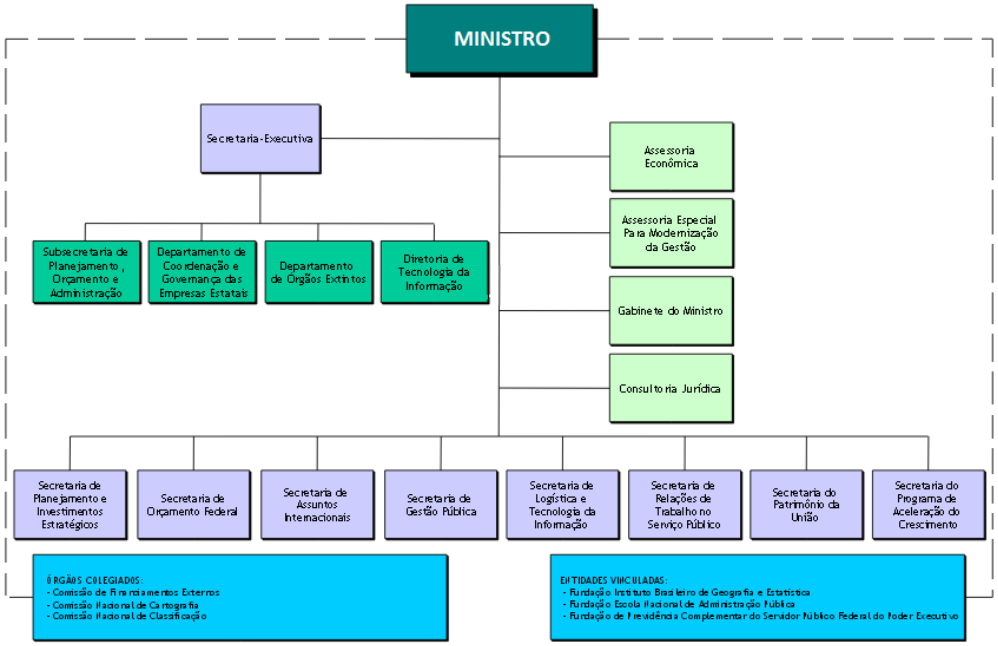
Entende e aceita.	115	60%
Questiona e tenta justificar.	37	19%
Busca maneiras de fazer mesmo assim.	7	4%
Busca apoio de sua chefia ou de níveis superiores.	34	18%

Essa questão objetivou mensurar o grau de resistência os colaboradores em relação a restrições e controles provenientes de procedimentos de segurança da informação. Sabe-se que mudanças na cultura organizacional, incluindo a forma como as pessoas trabalham, nem sempre são recebidas positivamente. As mudanças no ambiente corporativo englobam alterações fundamentais no comportamento humano, dos padrões de trabalho e nos valores em resposta a modificações ou antecipando alterações estratégicas, de recursos ou de tecnologia. Um dos fatores cruciais para o processo de mudança é o gerenciamento das pessoas, mantendo alto nível de motivação e evitando desapontamentos. O grande desafio não é a mudança tecnológica em si, mas mudar pessoas e a cultura organizacional, renovando os valores para ganhar vantagem competitiva (HERZOG *apud* ROSSI, 2000)

Assim, mais de 60% dos entrevistados respondeu compreender e aceitar bloqueios relativos à segurança da informação. Um total de 19% respondeu que questiona o bloqueio e tenta justificar. Um ponto importante relativo à segurança da informação é que seus procedimentos não devem engessar o negócio, portanto, é normal que surjam situações passíveis de questionamento quando de bloqueios em ambientes corporativos. Departamentos de *marketing* e media não deveriam ter os mesmos bloqueios de departamentos administrativos, por exemplo. Enriquecendo essa análise, cerca de 18% respondeu que busca apoio de sua chefia ou níveis superiores quando se deparam com um bloqueio proveniente de segurança da informação. Esse dado permite duas linhas de raciocínio: a primeira poderia refletir no fato da necessidade de determinado acesso/ação em detrimento de atividades profissionais que realmente requerem um acesso mais privilegiado. A segunda pode refletir o uso de influência sem fins profissionais para ter um acesso mais

privilegiado. Ambos estão relacionados ao poder que os níveis dentro de um organograma têm sobre outros. Analise o cenário hipotético abaixo:

Figura 12: Cenário hipotético



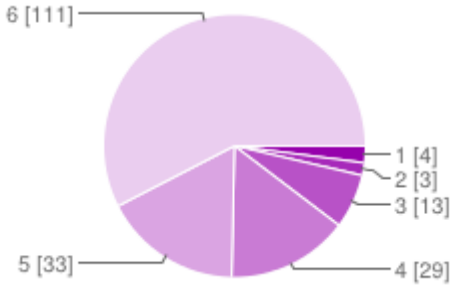
Fonte: Desenvolvido pelo autor em 2014

A diretoria de tecnologia da informação teria menos poder de articulação do que a Assessoria Econômica, por exemplo, na aprovação de algum procedimento que influenciasse na cultura da organização. No caso do Ministério da Justiça a Diretoria de Tecnologia da Informação está há apenas 1 nível do Ministro – a autoridade máxima do órgão. Em alguns outros ministérios como o Ministério do Desenvolvimento Agrário, a área de tecnologia da informação não é uma diretoria e está abaixo ainda da Subsecretaria de Gestão, Orçamento e Administração, ou seja, a dois níveis do ministro. Apesar dos procedimentos muitas vezes serem aprovados pelo próprio gabinete do ministro e terem validade para toda a organização, não há força política suficiente e capaz de mudar a cultura da organização em função da proeminência e influência de níveis mais altos e poderosos.

Finalmente, apenas 4% dos entrevistados assinalou que tentariam buscar maneiras de burlar os procedimentos de bloqueio por conta própria.

6- 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)

Figura 13: Pontuação de importância da segurança da informação.



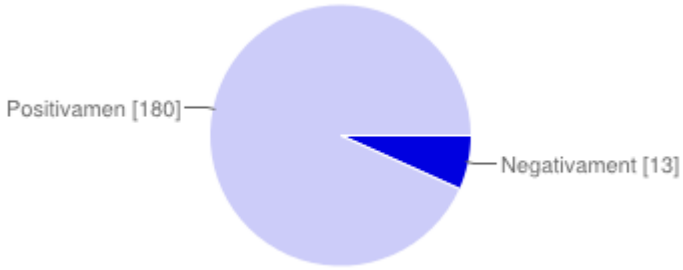
1	4	2%
2	3	2%
3	13	7%
4	29	15%
5	33	17%
6	111	58%

Fonte: Desenvolvido pelo autor em 2014.

Em relação à intensidade de importância que a segurança da informação tem para suas atividades, a grande maioria, com 58% respondeu que a importância tem intensidade muito alta, ou seja 6, em seguida, 17% respondeu que tem intensidade de alta para média e 15% que tem intensidade média para alta com 4. Para 7% a segurança da informação tem importância de média para baixa, marcando a intensidade 3, e com intensidades baixa para média com 2% e muito baixa, também com 2%. Percebe-se que para grande maioria, a segurança da informação tem relevância em suas atividades profissionais.

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

Figura 14: Cenário hipotético.



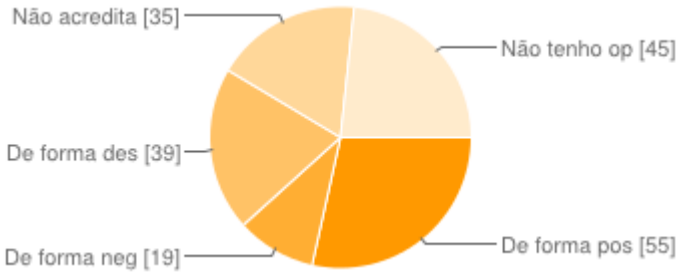
Negativamente	13	7%
Positivamente	180	93%

Fonte: Desenvolvido pelo autor em 2014.

Um total de 93% dos entrevistados respondeu acreditar que os procedimentos de segurança da informação impactam de forma positiva em seu trabalho e apenas 7% respondeu que eles impactam negativamente. Esse dado pode representar uma expectativa positiva dos colaboradores do Ministério da Justiça em relação à segurança da informação. Mesmo que na questão 2 tenha sido identificado que os colaboradores, 47% , não tenham conhecimentos sobre normativos de informática, grande parte deles acredita que a segurança da informação tenha um impacto positivo em seu trabalho e grande parte a considera importante para o desenvolvimento de suas atividades profissionais, conforme observado na questão 6. Dessa forma, pode-se inferir que o investimento em educação e treinamento nas disciplinas voltadas a segurança da informação no âmbito do Ministério da Justiça podem ter um efeito positivo para uma melhor compreensão e conscientização dos servidores desse órgão.

8 - Na sua percepção, como os funcionários do MJ entendem as ações e procedimentos de Segurança da Informação?

Figura 14: Percepção dos colaboradores



Fonte: Desenvolvido pelo autor em 2014.

De forma positiva	55	28%
De forma negativa	19	10%
De forma desconfiada	39	20%
Não acreditam que possa trazer benefício	35	18%
Não tenho opinião	45	23%

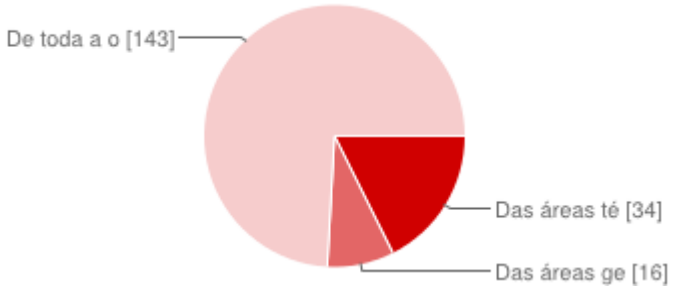
Enquanto na questão anterior o objetivo foi mensurar o impacto dos controles e procedimentos de Segurança da Informação nas atividades profissionais dos colaboradores, o objetivo dessa questão foi mensurar a impressão que o respondente tem em relação a como os colaboradores de forma geral veem esses controles de segurança da informação no Ministério da Justiça.

Apesar de 93% ter respondido acreditar que a segurança da informação tem impacto positivo sobre seu trabalho, apenas 28% aqui acreditam que os funcionários do Ministério da Justiça entendem positivamente os controles de procedimentos de segurança da informação. É perceptível a diferença proveniente da nuance da questão e disponibilizando maiores opções de resposta. Do total, 20% disseram acreditar que os colaboradores do MJ veem a segurança da informação de forma desconfiada, o que talvez reflita uma deficiência no esclarecimento do que é e para que serve a segurança da informação. O mesmo se aplica para os 18% que

responderam que os colaboradores não acreditam que de fato possa trazer algum benefício. Caso o MJ, por exemplo, divulgasse relatórios de tratamento de incidentes como o CTIR, citado na questão 3, provavelmente esse percentual seria menor, uma vez que os resultados seriam conhecidos. Apenas 10% do total respondeu acreditar que a segurança da informação é entendida de forma negativa pelos colaboradores, o que está bem próximo dos 7% obtidos na questão anterior.

9 - Você acredita que a responsabilidade por segurança da informação é de competência:

Figura 15: Responsabilidade pela segurança da informação.



Fonte: Desenvolvido pelo autor em 2014.

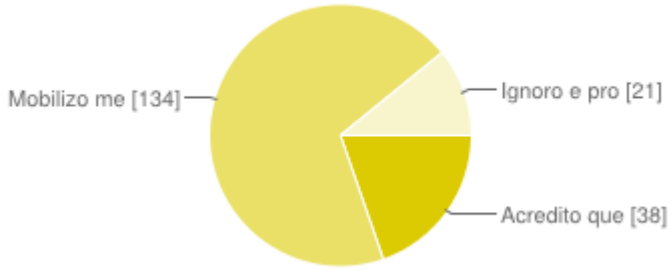
Das áreas técnicas de informática	34	18%
Das áreas gestoras da organização	16	8%
De toda a organização	143	74%

Uma percepção interessante dos 194 colaboradores respondentes foi os 74% que afirmaram entender que a segurança da informação é dever de todos dentro da organização, o que representa um caminho positivo para intensificação de políticas de conscientização e educação voltadas ao tema no âmbito do MJ. Um total de 18% acredita que a responsabilidade por segurança da informação seja das áreas de informática, o que não é um percentual estranho, uma vez que muitos controles nascem dessa área e que grande parte das ameaças conhecidas transita nesse

contexto. Apenas 8% acreditam que essa responsabilidade seja da área gestora do Ministério.

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

Figura 16: Comprometimento pela segurança da informação.



Fonte: Desenvolvido pelo autor em 2014.

Acredito que as coisas devam ser feitas da forma que sempre deram certo.	38	20%
Mobilizo meu pessoal/colegas para adequação às novas regras e procedimentos.	134	69%
Ignoro e procuro saber apenas quando for de meu interesse.	21	11%

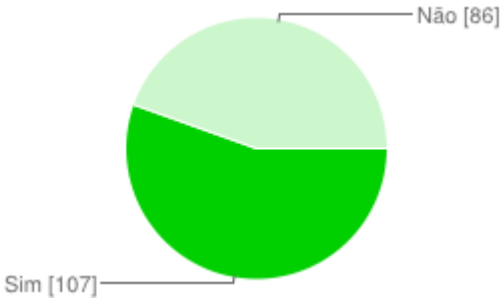
Essa questão visou avaliar o grau de em relação a novos e existentes procedimentos de segurança da informação. O grande total com 69%, respondeu mobilizar os colegas para que se adequem às novas regras e procedimentos de segurança da informação, o que pode demonstrar mais uma vez uma boa abertura dos colaboradores caso sejam bem orientados. O próximo item é compatível com os dados obtidos por aqueles que veem os procedimentos de segurança da informação, na questão 8, de forma desconfiada Aqui também, 20% respondeu acreditar que as coisas continuem sendo feitas da forma que sempre foram, o que representa uma certa resistência à mudanças que pode ser causada até mesmo

pela desconfiança em relação à esses novos procedimentos e que pode significar uma boa oportunidade de atuação.

Apenas 11% do total de respondentes afirmou ignorar e procurar saber dos procedimentos apenas quando fosse de seu interesse.

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

Figura 17: Experiência com incidentes de segurança da informação.



Sim	107	55%
Não	86	45%

Fonte: Desenvolvido pelo autor em 2014.

Essa pergunta teve como objetivo mensurar o percentual de colaboradores respondentes que experimentaram incidentes de segurança da informação. Um grande percentual de 55%, mais da metade do total de entrevistados, respondeu já ter experimentado incidentes de segurança da informação dentro do âmbito do Ministério da Justiça. O número é significativo e remete à duas análises: a primeira é o fato positivo dos colaboradores terem entendido que passaram por um incidente de segurança, o que pode demonstrar um certo grau de maturidade em relação ao que é ou ao que não é uma atividade prevista no seu ambiente de trabalho. A segunda análise pode representar um dado negativo em que mais de 50% da amostra experimentou incidentes consumados dentro do ambiente do Ministério da Justiça, o que pode significar um termômetro para a melhoria de controles internos e

externos para tratamento de vulnerabilidades, ameaças, riscos e incidentes. O restante, formado por 45% do total, respondeu não ter experienciado incidentes de segurança da informação. O fato de 55% ter afirmado a experiência, pode levar a questionarmos o grau de consciência sobre o que é um incidente de segurança da informação desses 45%. No enunciado foram exemplificados tipos de incidentes de segurança da informação (e-mails solicitando senha, o acesso não autorizado a documentos ou sistemas, o uso de informações privilegiadas por pessoas não autorizadas). Hipoteticamente, se os 55% receberam, por exemplo, e-mails solicitando senha, é improvável que ninguém dos 45% não o tenham recebido também. Porém, trata-se de uma hipótese que pode servir como parâmetros para medidas informativas na organização.

CONSIDERAÇÕES FINAIS

Possíveis fatores que poderiam de alguma forma impactar na implantação de uma política de segurança da informação no Ministério da Justiça foram analisados sobre duas perspectivas: uma relativa à estrutura da organização e outra relativa à percepção dos colaboradores da organização sobre o tema em pauta.

Quando se fala em implantação de uma política de segurança da informação, ela deve deixar de ser apenas um documento para fins de conformidade por exigência de órgãos de regulação e devem realmente apoiar o negócio da organização, deve ser praticada no cotidiano e trazer resultados palpáveis.

Assim, vários fatores relativos à estrutura foram analisados e, para além de apenas um olhar superficial do organograma, pôde-se analisar fatores adicionais como manifestações dos colaboradores em relação às questões estruturais e ainda documentos que, dentre outros assuntos, exploraram o cenário estrutural do Ministério da Justiça e se revelaram realmente impactantes. Fatores esses, não somente relacionados à aplicação de uma política de segurança da informação, mas de quaisquer iniciativas que surjam da atual área de tecnologia da informação do Ministério da Justiça. Os principais fatores estruturais impactantes foram:

- **Posição da área de TI verticalmente no organograma atual:** a área de tecnologia da informação do Ministério da Justiça está estrategicamente mal posicionada no organograma, perdendo completamente o poder de persuasão em relação a níveis mais altos do ministério e sendo frequentemente influenciada por níveis exatamente superiores. São ao todo 4 (quatro) degraus no organograma vertical até chegar ao nível mais alto da organização, com subordinação à diversas áreas. Essa

característica foi inclusive observada pelo acórdão nº 1163/2008 do TCU, após auditoria realizada no órgão, que sugere que a área de TI esteja localizada de forma independente dos departamentos de usuários e a uma proximidade adequada da alta administração, de modo a possibilitar o estabelecimento de uma parceria entre eles. Como a segurança da informação transcende a área de tecnologia, e para fins dessa pesquisa, um bom começo seria criar uma área de segurança da informação, independente de TI, e posiciona-la estrategicamente próxima ao alto escalão.

- **Inexistência de uma área de Segurança da Informação desvinculada diretamente da área de Tecnologia da Informação e vinculada a áreas estratégicas:** para além do posicionamento pouco estratégico, não existe, pelo menos oficialmente, a menção a uma área de segurança da informação no organograma. Assim, o assunto é tratado como uma iniciativa de tecnologia da informação e não como uma preocupação organizacional, como um dever de todos.
- **Assuntos de Tecnologia da Informação tratados meramente como área meio e não estratégica:** por mais que muitos recursos de TI sejam *commodities*, faz-se necessário alinhar a TI, incluindo Segurança da Informação, ao negócio uma vez que ela pode contribuir com soluções e controles que apoiarão os objetivos organizacionais. Esse aspecto foi observado na matriz SWOT presente no PDTI 2013/2015 do Ministério da Justiça e torna-se estrutural uma vez que esse tipo de abordagem tem implicação no fluxo de aprovações de projetos e orçamentos dos níveis mais altos (estratégicos) para mais baixos (táticos/operacionais).

- **Falta de continuidade de papéis em cargos estratégicos pela falta de vínculo com a organização e questões políticas:** apesar de ampla e transgressora, a questão pede atenção pelo fato de impactar diretamente na continuidade e no sucesso de projetos iniciados, o que implica, pelo menos indiretamente, em uso de recursos público. Caso se faça uma análise minuciosa, a descontinuidade de projetos caracterizaria, no mínimo, mal uso de dinheiro público. Para questões do tipo, a existência de uma área de controladoria interna ligada aos objetivos estratégicos da organização seria altamente positiva, uma vez que, por mais utópico que seja sugerir a diminuição de trocas de cargos públicos, uma controladoria interna garantiria o monitoramento do cumprimento de projetos, políticas e programas baseados no investimentos provenientes de diretrizes pré-aprovadas de planejamento estratégico. Sugere-se a utilização de melhores práticas como o próprio COBIT, citado no referencial teórico, para alinhar segurança da informação e TI ao negócio, de forma a prover controle e aderência a objetivos estratégicos de curto, médio e longo prazo e promover uma responsabilização por esses objetivos. Isso significa que mesmo que posições estratégicas se alternem, elas saberão que devem promover a continuidade estratégica da área em harmonia com os objetivos de alto nível da organização.

- **Interferências políticas externas que impactam no planejamento estratégico interno:** este aspecto identificado como uma ameaça no Plano Diretor de Tecnologia da Informação 2013/2015 do Ministério da Justiça corrobora com o fato do posicionamento pouco estratégico da área de tecnologia da informação e traz a tona o pouco comprometimento e

envolvimento do alto escalão da organização com as iniciativas de tecnologia da informação. Tanto as normas da família ISO 27.000 quanto o framework COBIT afirmam que o envolvimento do alto escalão na aplicação das boas práticas de governança e segurança da informação é de extrema importância para o seu sucesso. A existência de controladoria interna, tratando a aprovação de políticas e projetos, endossada também pelo alto escalão e associada a uso de recursos públicos, poderia ser uma boa estratégia com o objetivo de forçar uma atenção maior dos níveis estratégicos para questões de segurança da informação.

- **Falta de força do comitê de segurança da informação:** apesar de instituído, em função de todos os fatores observados, percebe-se que se trata de um comitê meramente formal. A citada auditoria do TCU observa que a falta de uma instância superior para definir as prioridades do setor de TI gera disputa interna entre os gestores do Ministério desejosos de primazia nos trabalhos que gerenciam, indo de encontro ao problema estrutural analisado nos itens anteriores.

Em relação á avaliação quanto à percepção cultural dos colaboradores em relação ao tema segurança da informação, obtiveram-se resultados dos mais variados. A maior parte dos respondentes foi formada por servidores públicos, o que demonstra receio, desconhecimento ou falta de interesse pelo tema por parte de terceirizados, consultores e estagiários. É importante frisar que muitas dessas pessoas manipulam informações sensíveis relativas ao órgão no dia a dia, portanto, deve-se ampliar o grau de envolvimento com o tema segurança da informação para todos os colaboradores da organização. De forma a corroborar com o tema, logo na questão 02, praticamente a metade dos colaboradores respondentes declararam

desconhecer normativos de informática do Ministério da Justiça, isso representa um desconhecimento considerável em relação ao que o órgão espera de seus colaboradores em relação ao uso de recursos computacionais, o que envolve, dentre outros: uso de senha, uso de informações de sistemas corporativos, uso da internet e e-mails, uso de recursos computacionais, uso de softwares e equipamentos pessoais, responsabilidades, direitos e deveres enquanto funcionário.

Percebeu-se que os colaboradores tem uma consciência relativa sobre a importância de controles lógicos e físicos, uma vez que perguntas similares foram feitas de formas diferentes e obtiveram-se resultados igualmente diferentes. Essa constatação indica que eles trazem esses conceitos do mundo exterior, com pouco significado prático para as atividades do Ministério da Justiça. Em relação a tecnologias e recursos utilizados no dia a dia, as respostas foram bem divididas e alguns resultados com menos significância como backup de dados e instalação de software podem ser melhores explorados pela organização dentro das premissas descritas nas normas da família 27001 e melhores práticas de governança de TI como ITIL e COBIT de forma a conscientizar os colaboradores de seus direitos, deveres, limites e possibilidades. Um ponto recomendável de partida seria criar campanhas de informação em relação a controles de acesso físico e lógico, uso de senhas, melhores práticas de segurança da informação, direitos e deveres, baseados na política de segurança da informação e seus documentos complementares. Cartilhas informativas e manuais a serem lidos e preenchidos na admissão de novos colaboradores também contribuiriam para um aumento do conhecimento e comprometimento dos colaboradores em relação ao tema.

Em relação à análise de cultura quanto à percepção em relação aos controles impostos pela segurança da informação e o impacto dela no cotidiano do trabalho,

percebe-se que a maioria dos colaboradores enxerga como positiva e crê que possa trazer benefícios. Esse fato sugere uma abertura dos colaboradores para questões relativas ao tema segurança da informação, podendo-se inferir que culturalmente o impacto de políticas, controles e procedimentos de segurança da informação não seria recebido de forma tão negativa pelos colaboradores.

A análise do aspecto cultural permitiu o cruzamento com alguns resultados da análise estrutural, principalmente no que tange a opinião dos colaboradores sobre a efetividade dos procedimentos de segurança da informação, comumente guiados pela política de segurança da informação. Na quinta questão, sobre como os colaboradores procedem em casos de controles/bloqueios em relação à segurança da informação, muitos responderam que buscam apoio de suas chefias para realizar o que querem. Esse fato está diretamente ligado à posição da CGTI no organograma e aprofunda a análise sobre dificuldade de aplicação da POSIC por questões de subordinação administrativa decorrente de mal posicionamento da área.

Outro fator a ser observado é que, apenas 28% dos respondentes, acredita que os funcionários do Ministério da Justiça de forma geral entendem as ações de segurança da informação de forma positiva. Todo o restante ficou dividido entre a descrença no benefício, a visão negativa, falta de opinião e da visão desconfiada dessas ações. Isso vai de encontro a uma fraqueza identificada no PDTI 2013/2015, citado na análise das estruturas, que se refere à percepção negativa dos usuários em relação aos serviços prestados pela área de tecnologia da informação que está diretamente ligada à assuntos de segurança da informação.

Ou seja, faz-se necessário um movimento interno e com o apoio do alto escalão a fim de trabalhar essa visão cultural da tecnologia da informação, abrindo

um canal de conscientização, comprometimento e exibição de resultados que tornem palpáveis os controles derivados da política de segurança da informação.

Assim, por mais que o Ministério da Justiça esteja em conformidade com as exigências dos órgãos de controle tendo a política de segurança da informação e o comitê de segurança da informação instituído, os fatores relativos à sua estrutura, corroborados por alguns resultados de percepção cultural, impactam negativa, direta e indiretamente na aplicação de fato dessa política. Percebe-se que os fatores relativos à estrutura organizacional tem um impacto maior na implantação da política até porque é dali que partem as iniciativas de mudança organizacional, o que seria diretamente refletido na percepção dos colaboradores, configurando-se uma relação de causa e efeito.

O objetivo da pesquisa foi alcançado uma vez que foram identificados gargalos provenientes de uma profunda análise estrutural e que impactam na aplicação da política de segurança da informação, assim como foi possível captar a percepção dos colaboradores sobre o tema, obtendo-se uma visão de dupla perspectiva – uma estratégica e outra operacional – e chegando a um cenário no qual se percebeu quais são os aspectos de maior impacto na aplicação da política de segurança da informação na organização e como isso é refletido culturalmente na organização.

Para trabalhos futuros sugere-se um estudo mais aprofundado sobre o posicionamento estratégico da área de segurança da informação nos órgãos da administração pública federal, sobre formas de divulgação e educação de temas relacionados à segurança da informação num contexto de organizações públicas, considerando a alta rotatividade de funcionários, e principalmente, formas de garantir o comprometimento dos gestores e alto escalão com a segurança da

informação através de controles internos, prestação de contas e divulgação de resultados.

REFERÊNCIAS

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

ABNT. ABNT NBR ISO/IEC 27001:2006: Tecnologia da Informação - Técnicas de segurança - Sistemas de gestão de segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2006.

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.

BEAL, Adriana. *Segurança da informação:* princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005. 180 p.

BRASIL. *Decreto Nº 6.061, de 15 de março de 2007*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Ministério da Justiça, e dá outras providências. disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6061.htm>. Acesso em: 27 set. 2013.

BRASIL. Ministério da Justiça. *Cartilha para Emendas Orçamentárias*. 2013. Disponível em: <http://www.justica.gov.br/Acesso/acoes-e-programas/arquivos-anexos/2013-cartilha-de-emendas-parlamentares-1.pdf>. Acesso em: 20 fev. 2014.

BRASIL. Ministério da Justiça. *Portaria nº 3530 de 03 de Dezembro de* 2013. Institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça, e dá outras providências. Disponível em: <http://www.diariodasleis.com.br/>. Acesso em: 10 out. 2013.

BRASIL. *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. Disponível em: <http://www.lexml.gov.br/>. Acessado em: 13 abr. 2014.

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: 28 fev. 2013.

BRASIL. Tribunal de Contas da União. *Acórdão nº 1.163/2008*. Plenário. Relator: Ministro Benjamin Zymler. Sessão de 18/06/2008. Diário Oficial da União, Brasília, DF, 24 jul. 2018

BRASIL. Departamento de Segurança de Informação e Comunicações. Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal. *Estatísticas referentes ao segundo trimestre de 2014*. 2014. Disponível em: < www.ctir.gov.br/estatisticas.html>. Acesso em: 19 set. 2014.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. *Instrução normativa nº 4, de 12 de novembro de 2010*

(IN04). Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. 2010c. Disponível em :<http://www.governoeletronico.gov.br/biblioteca/arquivos/instrucao-normativa-no-04-de-12-de-novembro-de-2010/download>. Acesso em: 28 jul. 2013.

BRASIL. *Instrução Normativa GSI/PR 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. Disponível em: < http://www.governoeletronico.gov.br/anexos/>. Acesso em 26 abr. 2014.

BRASIL. Ministério da Justiça. Coordenação Geral de Tecnologia da Informação. *Plano Diretor de Tecnologia da Informação 2013/2015*. 2013.

BRASILEIRO, Alice de Barros Horizonte. *Rebatimento espacial de dimensões socioculturais:* Ambientes de trabalho. Rio de Janeiro: UFRJ/FAU. 2007.

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.

Trenzinho Federal. *ISTO É INDEPENDENTE*. Brasil, 02 de abril de 2002, atualizado em 10 de Abril de 2013. 1697, pág. 34 -36.

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

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: 20 jul. 2013.

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

DAYCHOUW, Merhi. *40 Ferramentas e Técnicas de Gerenciamento*. 3. ed. Rio de Janeiro: Brasport, 2007.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. *Implantando a governança de TI:* da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

FERREIRA, Fernando Nicolau Freitas. *Segurança da Informação.* Rio de Janeiro: Ciência Moderna, 2003.

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

GIL, Antônio Carlos. *Métodos e técnicas de pesquisa social.* 5. ed. São Paulo: Atlas, 2007.

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

ISACA. *COBIT 5:* A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, 2012, 94 p.

IT GOVERNANCE INSTITUTE. *COBIT 4.1:* Control Objectives, Management Guidelines and Maturity Models. USA, 2007.

KWASNICKA, E. L.. *Introdução à Administração.* 6 Ed. São Paulo: Editora Atlas, 2007

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

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

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

NOGUEIRA, Fernando do Amaral. *Continuidade e Descontinuidade Administrativa em Governos Locais:* Fatores que sustentam a ação pública ao longo dos anos. São Paulo: Dissertação de Mestrado em Administração da FGV, 2006.

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

PINHEIRO, Patrícia Peck. *Direito digital.* São Paulo: Saraiva, 2009

PIRES, José Calixto de Souza; MACÊDO, Kátia Barbosa. *Cultura organizacional em organizações públicas no Brasil.* Revista de Administração Pública, 2006, 40. Disponível em: <http://www.redalyc.org/articulo.oa?id=241016430005>. Acesso em 3 oct. 2014.

Pontes, Edison. *Políticas e normas para segurança da informação.* Rio de Janeiro: Brasport, 2012.

ROSSI, Luiz Carlos. *Mudança organizacional e competitividade:* um estudo de caso em empresa de telecomunicações. Dissertação de mestrado. Universidade Federal do Rio Grande do Sul. 2000.

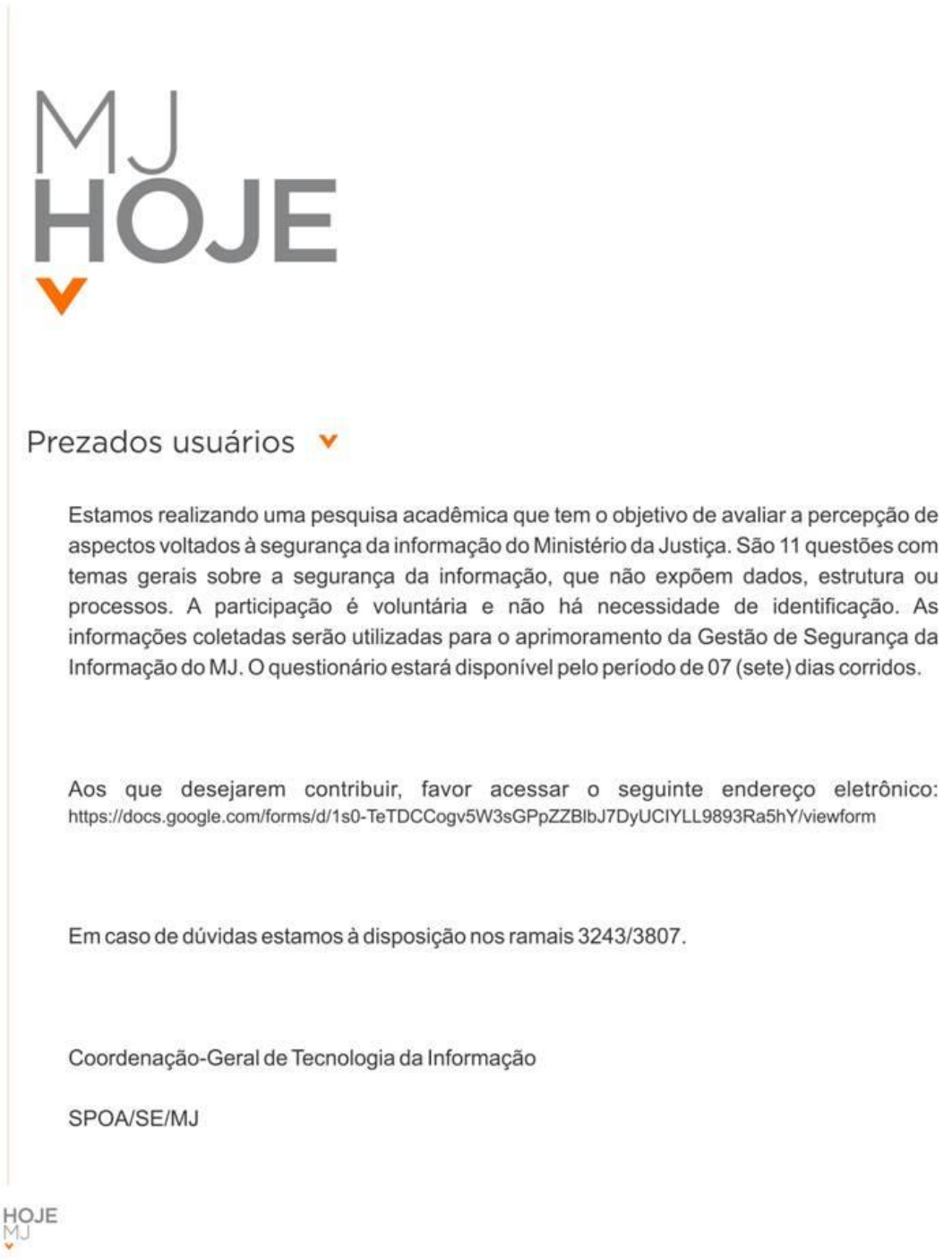
SEMOLA, M. *Gestão da segurança da informação.* Rio de Janeiro: Campus, 2003.

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/>. Acesso em: 25 out. 2013.

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.

APÊNDICE A - QUESTIONÁRIO



MJ HOJE

Prezados usuários

Estamos realizando uma pesquisa acadêmica que tem o objetivo de avaliar a percepção de aspectos voltados à segurança da informação do Ministério da Justiça. São 11 questões com temas gerais sobre a segurança da informação, que não expõem dados, estrutura ou processos. A participação é voluntária e não há necessidade de identificação. As informações coletadas serão utilizadas para o aprimoramento da Gestão de Segurança da Informação do MJ. O questionário estará disponível pelo período de 07 (sete) dias corridos.

Aos que desejarem contribuir, favor acessar o seguinte endereço eletrônico: https://docs.google.com/forms/d/1s0-TeTDCCogv5W3sGPpZZBlbJ7DyUCIYLL9893Ra5hY/viewform

Em caso de dúvidas estamos à disposição nos ramais 3243/3807.

Coordenação-Geral de Tecnologia da Informação

SPOA/SE/MJ

HOJE MJ

Pesquisa Acadêmica - Ministério da Justiça

Prezado colaborador,

Este questionário tem por objetivo mensurar a percepção de aspectos voltados a segurança da informação no âmbito do Ministério da Justiça. 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.

*Obrigatório

1- Por favor, informe seu vínculo com o MJ: *

- Servidor
- Consultor
- Terceirizado

2- Você tem conhecimento de algum normativo/recomendações do MJ voltados a informática? *

- Sim
- Não

3 - Dos aspectos a seguir, qual você considera mais importante em termos de segurança institucional: *

- Manipulação de informações sigilosas
- Segurança física do ambiente de trabalho
- Acesso não autorizado de pessoas à ambientes do MJ
- Conteúdo digital sobre o MJ

4 - 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 da internet
- Utilização de computadores
- Uso das informações institucionais
- Realização de Backup’s
- Instalação de software’s
- Uso de senhas

- Nenhuma

5 - 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.

6- 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

7 - Você acredita que procedimentos voltados à Segurança da Informação impactam positiva ou negativamente no seu trabalho? *

- Negativamente
- Positivamente

8 - Na sua percepção, como os funcionários do MJ 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

9 - Você acredita que a área de segurança da informação é de competência: *

- Das áreas técnicas de informática
- Das áreas gestoras da organização
- 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/colegas 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 MJ (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

Enviar

ANEXO B – QUADRO COM DISPOSITIVOS LEGAIS

Quadro dos dispositivos legais de Caráter Federal, relacionados à segurança da informação[3]:

Dispositivo	Mandamento Legal	Aspecto da SIC
Constituição Federal, art. 5º, inciso X.	Direito à privacidade.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XII.	Direito à privacidade das comunicações.	Sigilo dos dados telemáticos e das comunicações privadas.
Constituição Federal, art. 5º, inciso XIV.	Resguardo do sigilo profissional em caso de ofício que exige a ampla confidência no interesse de quem confidencia como advogados, padres, médicos, psicólogos, etc.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II.	Direito à informação e ao acesso aos registros públicos.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 5º, inciso XXXIV.	Direito de petição e de obtenção de certidões em repartições públicas.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 23, incisos III e IV.	Dever do Estado de proteger os documentos e obras.	Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
Constituição Federal, art. 216, § 2º.	Obrigação da Administração Pública de promover a gestão documental.	Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.
Constituição Federal, art. 37, caput.	Vinculação da Administração Pública aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.	Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.
Constituição Federal, art. 37, § 6º.	Responsabilidade objetiva do Estado e das pessoas de direito	Responsabilidade objetiva do Estado por dano

[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>

Código Civil, arts. 927 e 932caput, III.	privado prestadoras de serviços públicos pelos danos causados a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.	decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.
Constituição Federal, art. 37, § 7º.	Lei disporá sobre os requisitos e as restrições ao ocupante de cargo ou emprego da administração direta e indireta que possibilite o acesso a informações privilegiadas.	Necessidade de regulamentação do acesso a informações privilegiadas.
Consolidação das Leis do Trabalho - CLT, art. 482, alínea g.	Rescisão de contrato de trabalho de empregado que viola segredo da empresa.	Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).
Código de Conduta da Alta Administração, art. 5º, § 4º.	Caráter sigiloso das informações pertinentes à situação patrimonial da autoridade pública.	Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).
Código de Conduta da Alta Administração, art.14, inciso II.	Proibição da autoridade pública de prestar consultoria valendo-se de informações não divulgadas publicamente a respeito de programas ou políticas do órgão ou da entidade da Administração Pública Federal a que esteve vinculado ou com que tenha tido relacionamento direto e relevante nos seis meses anteriores ao término do exercício de função pública.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II.	Proibição de alteração de documentos que devam ser encaminhados para providências.	Proteção da integridade das informações públicas.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea "l" do inciso XV da Seção II.	Proibição de retirar da repartição documento ou qualquer outro bem.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso X da Seção I.	Deixar o servidor público ou qualquer pessoa à espera de solução que compete ao setor em que exerça suas funções, permitindo a formação de longas filas, ou qualquer outra espécie	Proteção da disponibilidade das informações públicas.

	de atraso na prestação do serviço, não caracteriza apenas atitude contra a ética ou ato de desumanidade, mas principalmente grave dano moral aos usuários dos serviços públicos.	
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso VII da Seção I.	Obrigação moral de conferir publicidade aos atos administrativos, salvo os sigilosos.	Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso IX da Seção I.	Causar dano a qualquer bem pertencente ao patrimônio público, deteriorando-o, por descuido ou má vontade, não constitui apenas uma ofensa ao equipamento e às instalações ou ao Estado, mas a todos os cidadãos.	Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II.	Dever de aperfeiçoar o processo de comunicação com os usuários para bem servi-los.	Disponibilidade das comunicações.
Código de Defesa do Consumidor, arts. 43 e 44.	Direito de acesso do consumidor às suas informações pessoais arquivadas em bancos de dados e direito de retificação das informações incorretas.	Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.
Código Penal, art. 151.	Pena de detenção de 1 a 6 meses ou multa por crime de violação de correspondência fechada dirigida a outrem, sonegação ou destruição de correspondência, e violação de comunicação telegráfica, radioelétrica ou telefônica.	Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.
Código Penal, art. 152.	Pena de detenção de 3 meses a dois anos pelo crime de desvio, sonegação, subtração, supressão ou revelação de conteúdo de correspondência comercial, abusando da condição de sócio ou empregado.	Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.
Código Penal, art. 153, § 1º-A.	Pena de 1 a 4 anos e multa por crime de divulgação de documento confidencial contido ou não nos sistemas ou bancos de dados da Administração Pública.	Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.

Código Penal, art. 154.	Pena de 3 meses a um ano, ou multa por crime de violação de segredo profissional.	Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.
Código Penal, art. 154-A.	Pena - detenção, de 3 meses a 1 ano, e multa.	Proteção à violação de equipamentos e sistemas - sejam eles conectados ou não à internet - com intenção de destruir dados ou informações, ou instalar vulnerabilidades.
Código Penal, art. 184, § 3º.	Pena de 2 a 4 anos por crime de violação de direito autoral mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema.	Proteção da autenticidade.
Código Penal, art. 266, § 1º e 2º.	Pena - detenção, de 1 mês a 1 ano, ou multa.	Proteção a não interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.
Código Penal, art. 297.	Pena de 2 a 6, e multa por crime de falsificação de documento público.	Proteção da integridade e autenticidade dos documentos públicos.
Código Penal, art. 298.	Pena de 1 a 5 anos, e multa por crime de falsificação de documento particular.	Proteção da integridade e autenticidade dos documentos particulares.
Código Penal, art. 298, Parágrafo Único.	Pena de 1 a 5 anos, e multa por crime de falsificação de cartão.	Proteção da integridade e autenticidade dos cartões.
Código Penal, art. 305.	Pena de 2 a 6 anos e multa por crime de supressão, destruição ou ocultação de documento públicoou particular.	Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 307.	Pena de 3 meses a 1 ano, ou multa por crime de falsa identidade.	Proteção da autenticidade.
Código Penal, art. 311-A.	Pena de 1 a 6 anos, aumentada em 1/3 se for cometido por Funcionário Público.	Proteção ao sigilo dos certames de interesse público.
Código Penal, art. 313-A.	Pena de 2 a 12 anos e multa por crime de inserção de dados falsos em sistema informatizado ou banco de dados da Administração	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades

	Pública, alteração ou exclusão de dados corretos.	públicos.
Código Penal, art. 313-B.	Pena de 3 meses a 2 anos e multa por crime de modificação ou alteração não autorizada de sistemas de informações.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 314.	Pena de 1 a 4 anos por crime de extravio, sonegação ou inutilização de livro ou documento de que tem a guarda em razão do cargo.	Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 325.	Pena de 2 meses a 6 anos, ou multa por crime de violação de sigilo funcional.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Código Processo Penal, art. 20.	Sigilo do inquérito policial	Proteção de informações sigilosas.
Código Processo Penal, art. 207.	Proibição de depor das pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho.	Proteção do sigilo profissional.
Código Processo Penal, art. 745.	Sigilo do processo de reabilitação do condenado.	Proteção de informações sigilosas relacionadas ao condenado.
Código Tributário Nacional, art. 198.	Proibição de divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.	Proteção do sigilo fiscal.
Código de Processo Civil, art. 347, inciso II c/c art. 363, inciso IV.	Direito da parte de guardar sigilo profissional.	Proteção da privacidade de seus clientes.
Código de Processo Civil, art. 406, inciso II c/c art. 414, § 2º.	Direito da testemunha de guardar sigilo profissional.	Proteção da privacidade de seus clientes.
Lei nº 6.538/78, art. 5º.	Direito a inviolabilidade dos serviços postais e de telegramas.	Sigilo da correspondência.
Lei nº 6.538/78, art. 41.	Pena de detenção de 3 meses a 1 ano, ou multa por violação de sigilo profissional por	Proteção da privacidade de correspondência.

	funcionário do serviço postal.	
Lei nº 7.170/83, art. 13.	Pena de 3 a 15 anos por crime espionagem ou divulgação de informações sigilosas a grupo estrangeiro, ou a organização ou grupo de existência ilegal.	Proteção das informações sigilosas relacionadas à segurança nacional
Lei nº 7.232/84, art. 2o, inciso VIII.	Exigência de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados informatizados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas.	Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.
Lei nº 7.492/86, art. 18.	Pena de reclusão de 1 a 4 anos e multa por crime de violação de sigilo bancário.	Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.
Lei nº 8.027/90, artigo 2º, inciso V, alínea "a" e inciso VII.	Deveres do Funcionário Público Civil.	Proteção às informações protegidas pelo sigilo.
Lei nº 8.027/90, artigo 5º, inciso I.	Pena de demissão para o servidor que se valer ou permitir dolosamente que terceiros tirem proveito de informação obtida em função do cargo, para lograr, proveito pessoal ou de outrem.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Lei nº 8.027/90, art. 5º, parágrafo único, inciso V.	Pena de demissão para o servidor que revelar segredo de que teve conhecimento em função do cargo ou emprego.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei nº 8.112/90, art. 116, inciso VIII.	Dever do servidor de guardar sigilo sobre assunto da repartição.	Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.
Lei nº 8.112/90, art. 132, inciso IX.	Pena de demissão para o servidor que revelar segredo do qual se apropriou em razão do cargo ou função pública.	Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.
Lei nº 8.137/90, art. 3º, inciso I.	Constitui crime funcional contra a ordem tributária punido com pena de 3 a 8 anos e multa extraviar livro oficial, processo fiscal ou qualquer documento, de que tenha a guarda em razão da	Proteção da disponibilidade de informações para manutenção da ordem tributária.

	função; sonegá-lo, ou inutilizá-lo, total ou parcialmente, acarretando pagamento indevido ou inexato de tributo ou contribuição social.	
Lei nº 8.429/92, art.11, incisos III, IV e VII.	Constitui ato de improbidade administrativa revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo; negar publicidade aos atos oficiais; e revelar ou permitir que chegue ao conhecimento de terceiro, antes da respectiva divulgação oficial, teor de medida política ou econômica capaz de afetar o preço de mercadoria, bem ou serviço.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.
Lei nº 8.429/92, art. 13.	Dever do agente público de apresentar anualmente sua declaração de bens e valores que integram o seu patrimônio pessoal a fim de ser arquivada no serviço de pessoal competente e pena de demissão para o servidor que se recusar a prestar tal informação ou que a prestar falsa.	Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.
Lei nº 8.443/92, art. 86, inciso IV.	Dever do servidor que exerce funções específicas de controle externo no TCU de guardar sigilo sobre dados e informações obtidos em decorrência do exercício de suas funções e pertinentes aos assuntos sob sua fiscalização, utilizando-os, exclusivamente, para a elaboração de pareceres e relatórios destinados à chefia imediata.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei Complementar nº 75/93, art. 8º incisos II, VIII e §§ 1º e 2º.	Competência do Ministério Público da União para requisitar informações, exames, perícias e documentos de autoridades da Administração Pública direta ou indireta e ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública, bem como a responsabilização pelo uso dessas informações.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

Lei nº 8.625/93, art. 26, inciso I, alínea "b" e inciso II.	Competência do Ministério Público de requisitar informações, exames periciais e documentos de autoridades federais, estaduais e municipais, bem como dos órgãos e entidades da administração direta, indireta ou fundacional, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e requisitar informações e documentos a entidades privadas, para instruir procedimentos ou processo em que oficie.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei nº 8.906/94, art. 7º, inciso XIX.	Direito do advogado de resguardar o sigilo profissional.	Proteção da privacidade do cliente do advogado.
Lei nº 9.100/95, art. 67, incisos VII e VIII.	Constitui crime de fraude eleitoral nas eleições municipais as condutas de: (a) obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos (Detenção de 2 a 6 meses); e (b) tentar desenvolver ou introduzir comando, instrução ou programa de computador, capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados utilizado pelo serviço eleitoral (Reclusão de 3 a 6 anos).	Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.
Lei nº 9.279/96, art. 75.	O pedido de patente originário do Brasil cujo objeto interesse à defesa nacional será processado em caráter sigiloso.	Sigilo das patentes de interesse da defesa nacional.
Lei nº 9.279/96, art. 195, inciso XI.	Constitui crime de concorrência desleal divulgar, explorar ou utilizar, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que	Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.

	sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato.	
Lei nº 9.296/96, art. 10.	Pena de dois a quatro anos, e multa por crime de interceptação de comunicações telefônicas, de informática ou telemática, ou quebra de segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.	Sigilo dos dados e das comunicações privadas.
Lei nº 9.472/97, art. 3º, inciso V.	O usuário de serviços de telecomunicações tem direito à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas.	Sigilo das comunicações.
Lei nº 9.472/97, art. 3º, inciso VI.	O usuário de serviços de telecomunicações tem direito à não divulgação, caso o requeira, de seu código de acesso.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.472/97, art. 3º, inciso IX.	O usuário de serviços de telecomunicações tem direito ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.504/97, art. 72.	Pena de 5 a 10 anos pelas condutas de obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; desenvolver ou introduzir comando, instrução, ou programa de computador capaz de provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.	Proteção da integridade das informações de caráter eleitoral e dos equipamentos.
Lei nº 9.605/98, art. 62.	Pena de 1 a 3 anos e multa pela conduta de destruir, inutilizar ou deteriorar arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar	Disponibilidade e integridade de dados e informações.

	protegido por lei, ato administrativo ou decisão judicial.	
Lei nº 10.683/03, art. 6º, inciso IV.	Prevê a competência do GSIPR de coordenar a atividade de segurança da informação.	Todos os aspectos da segurança da informação.
Lei n.º 10.703/03, arts. 1º, 2º e 3º, de 18 de julho de 2003.	Incumbe aos prestadores de serviços de telecomunicações na modalidade pré-paga, em operação no território nacional, manter cadastro atualizado de usuários. Os dados constantes do cadastro, salvo motivo justificado, deverão ser imediatamente disponibilizados pelos prestadores de serviços para atender solicitação da autoridade judicial, sob pena de multa por infração cometida.	Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.
Lei n.º 12.737/12, de 30 de novembro de 2012.	Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.	Todos os aspectos da segurança da informação.
Lei nº 12.965, de 23 abril de 2014. (Marco Civil da Internet).	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.	Segurança jurídica para os usuários da rede, sejam eles usuários, empresas, provedores e Administração Pública.
Lei nº 12.970, de 8 maio de 2014, Seção III.	Altera o Capítulo VI do Título III e o art. 302 e revoga os arts. 89, 91 e 92 da Lei no 7.565, de 19 de dezembro de 1986 - Código Brasileiro de Aeronáutica, para dispor sobre as investigações do Sistema de Investigação e Prevenção de Acidentes Aeronáuticos - SIPAER e o acesso aos destroços de aeronave; e dá outras providências.	Sigilo Profissional e Proteção à Informação em investigações de acidentes aéreos.
Decreto nº 3.505/00, art. 1º.	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.	Pressupostos básicos da segurança da informação.

Decreto nº 4.801/03, art. 1º, inciso X.	Atribuição da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, de formular políticas públicas e diretrizes, aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos no âmbito da segurança da informação.	Todos os aspectos da segurança da informação.
Decreto nº 5.483/05, arts. 3º e 11.	Dever do agente público de apresentar anualmente sua declaração de bens e valores que integram o seu patrimônio e dever de sigilo por parte da Administração Pública dessas informações.	Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.
Decreto nº 5.687/06, arts. 10 e 13 do Anexo.	Convenção das Nações Unidas contra a Corrupção aprovada pelo Congresso Nacional e promulgada pelo Decreto nº 5.687/06, segundo a qual, cada Estado signatário deve esforçar-se para implementar, entre outras, as seguintes medidas: art. 10: a) instaurar procedimentos ou regulamentações que permitam ao público em geral obter informação sobre a organização, o funcionamento e os processos de adoção de decisões de sua administração pública, com o devido respeito à proteção da intimidade e dos documentos pessoais; b) simplificar procedimentos administrativos a fim de facilitar o acesso do público às informações; c) dar publicidade às informações; - art. 13: a) aumentar a transparência e promover a contribuição da cidadania aos processos de adoção de decisões; b) garantir o acesso eficaz do público à informação.	Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.

Decreto nº 6.029/07, art 1º, inciso II.	O Sistema de Gestão da Ética do Poder Executivo Federal tem como um de seus objetivos contribuir para a implementação de políticas públicas tendo a transparência e o acesso à informação como instrumentos fundamentais para o exercício de gestão da ética pública.	Disponibilidade das informações constantes nos registros públicos
Decreto nº 6.029/07, art. 10.	Nos trabalhos das Comissões de Ética deverão ser observados os princípios da proteção à honra e à imagem do investigado, bem como proteção à identidade do denunciante, que deverá ser mantida sob reserva se este o desejar.	Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.
Decreto nº 6.029/07, art. 13.	Serão classificados como "reservados" os procedimentos de investigação de condutas antiéticas. Concluída a investigação e após a deliberação da Comissão de Ética, o processo deixará de ser "reservado".	Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.
Decreto nº 6.029/07, art. 22.	Comissão de Ética Pública manterá banco de dados de sanções aplicadas para fins de consulta antes de novas nomeações.	Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

Quadro da legislação específica de Caráter Federal relacionada à Segurança da Informação e Comunicações:

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.

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 9800, de 26 de maio de 1999.	Permite às partes a utilização de sistema de transmissão de dados para a prática de atos processuais.
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 nº 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 Infraestrutura 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 11.419, 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.
Lei nº 12.527 de 18 de novembro de 2011 (LAI).	Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.
Lei Nº 12.735, de 30 de novembro de 2012.	Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
Lei Nº 12.737, de 30 de novembro de 2012.	Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; 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 4.414, de 07 de outubro de 2002.	Altera o Decreto no 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
Decreto nº 4.522, de 17 de dezembro de 2002.	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.
Decreto nº 4.801, de 06 de agosto de 2003.	Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo.
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 5.450, 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 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.

Decreto nº 7.724 de 16 de maio de 2012.	Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII docaput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição.
Decreto nº 7.724 de 16 de maio de 2012.	Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII docaput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição.
Decreto nº 7.845, de 14 de novembro de 2012.	Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
Decreto nº 8.096, de 04 de setembro 2013.	Altera o Decreto nº 4.801, de 6 de agosto de 2003, que cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo.
Decreto nº 8.097, de 04 de setembro de 2013.	Altera o Decreto nº 3.505, de 13 de junho de 2000, para incluir a Secretaria-Geral da Presidência da República no Comitê Gestor da Segurança da Informação.
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 n° 132 do STM, de 02 de fevereiro de 2005.	Institui o "e-STM", sistema que permite o uso de correio eletrônico para a prática de atos processuais, no âmbito do Superior Tribunal Militar - STM.
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 Superior Tribunal de Federal - 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 23.370/11 do TSE, de 13 de dezembro de 2011.	Dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral nas eleições de 2012. (Propaganda Eleitoral na Internet - art. 18 a 25).
Resolução nº 23.404/14 do TSE, de 11 de fevereiro de 20114.	Dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral nas eleições de 2014. (Propaganda Eleitoral na Internet - art. 19 a 26).