

UNIVERSIDADE FEDERAL DE SANTA CATARINA  
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA  
CURSO DE SISTEMAS DE INFORMAÇÃO

ALEXANDRE HENRIQUE

GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO PARA DEFESA  
CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL

FLORIANÓPOLIS

2012

ALEXANDRE HENRIQUE

GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO PARA DEFESA  
CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Trabalho de Conclusão de Curso apresentado à disciplina de Projetos II – INE 5632, como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação na Universidade Federal de Santa Catarina.

Orientador: Prof. Dr. João Cândido Dovicchi

FLORIANÓPOLIS

2012

Alexandre Henrique

GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO PARA DEFESA  
CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Este Trabalho de Conclusão de Curso foi julgado adequado e aprovado em sua forma final para obtenção do grau de Bacharel em Sistemas de Informações da Universidade Federal de Santa Catarina.

Florianópolis, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_.

Orientador:

---

Prof. Dr. João Cândido Dovicchi

Banca avaliadora:

---

Prof. Dr. Luiz Fernando Jacintho Maia

---

Prof. Dr. Ricardo Pereira e Silva

*Dedico este trabalho aos irmãos da Igreja Presbiteriana da Trindade que se tornaram a minha família. Por todo o carinho e compreensão, mesmo nas minhas ausências durante a realização deste trabalho.*

## AGRADECIMENTOS

*Sou grato a Deus por iluminar meus olhos e meu caminho me dando forças e colocando em mim o desejo de lutar. A Ele toda Glória!*

*Aos meus pais, Maurício da Conceição Henrique e Regina Fátima de Aguiar. Sem o amor, zelo, dedicação não poderia obter o prazer de concluir mais esta etapa de minha vida.*

*Agradeço à minha avó, Maria de Fátima de Aguiar, por ser tão especial e querida. Seu exemplo de humildade e perseverança revigora minhas forças a cada jornada que enfrento. Nunca poderei retribuir tão grande cuidado que sempre teve por mim.*

*Á minha namorada, Natália de Oliveira Daud. É fonte de alegria. Sua presença me tranquiliza nos momentos difíceis e me ajuda a superar os desafios. Pelo bem que me faz.*

*Aos professores da UFSC, em especial ao meu orientador João Cândido Dovicchi, por aceitar exercer importante apoio para a presente realização; e aos membros da banca: Ricardo Pereira e Silva e Luiz Fernando Jacintho Maia, cujos conhecimentos e experiência imprimiram maior qualidade a este trabalho.*

*Aos companheiros mais presentes: Jean Paulo, Leonardo Freitas e Ercílio Nascimento. Pelos momentos compartilhados ao longo da maior parte da jornada acadêmica.*

*Não sabes, não ouviste que o eterno Deus, o SENHOR, o Criador dos fins da terra, nem se cansa, nem se fatiga? Não se pode esquadrihar o seu entendimento.*

*Faz forte ao cansado e multiplica as forças ao que não tem nenhum vigor.*

*Os jovens se cansam e se fatigam, e os moços de exaustos caem, mas os que esperam no SENHOR renovam as suas forças, sobem com asas como águias, correm e não se cansam, caminham e não se fatigam.*

*– Isaías 40: 28 – 31.*

## RESUMO

HENRIQUE, Alexandre. **Governança de segurança da informação para defesa cibernética da Administração Pública Federal**. 2012. 132p. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Departamento de Informática e Estatística, Universidade Federal de Santa Catarina.

**Orientador:** Prof. Dr. João Cândido Dovicchi

O presente trabalho tem como finalidade a realização de um estudo da Governança de Tecnologia de Informação para implantação na Administração Pública Federal (APF) na melhoria da sua infraestrutura de defesa cibernética. Foi empregado o método dedutivo, juntamente com pesquisa qualitativa e exploratória do referencial teórico, caracterizando-se por uma ampla revisão bibliográfica, para se alcançar os objetivos geral e específico. As principais normas e as melhores práticas de Governança foram utilizadas sob a ótica da segurança cibernética a fim de agregar novos conhecimentos para as estratégias de defesa cibernética APF. As percepções obtidas através dos tópicos estudados na revisão bibliográfica e na sessão de gestão de segurança da informação nos órgãos da APF evidenciaram a importância e as necessidades do assunto tratado, uma vez que há o interesse do próprio governo para que sejam atendidos os requisitos de segurança da informação. As melhores práticas de Governança reproduzidas pelo COBIT, ITIL, NBR ISO/IEC 17799:2005 e PMBOK formam um arcabouço legal e normativo para o direcionamento da Gestão de Segurança da Informação com o intuito de proteger as comunicações, bancos de dados da APF e principalmente as infraestruturas críticas. Apesar das crescentes ameaças e tentativas de ataques, a aplicação das boas práticas alinhadas ao objetivo da organização proporciona garantir a disponibilidade, integridade, confidencialidade e autenticidade dos sistemas de informação. Percebe-se que as constantes transformações no campo cibernético exigem aperfeiçoamentos das medidas de segurança na mesma velocidade ou em velocidade maior. De tal modo, considero contribuir colaborativamente com o presente trabalho para o avanço da Segurança Cibernética da APF.

**Palavras chave:** Defesa Cibernética. Governança de TI. Segurança da Informação. COBIT. ITIL. NBR ISO/IEC 17799:2005. PMBOK.

## ABSTRACT

The present study aims to conduct a study of the Governance of Information Technology for deployment in the Federal Public Administration in improving its infrastructure cyber defense. We employed a deductive method with qualitative exploratory study of the theoretical framework, characterized by a broad literature review, to achieve the general and specific objectives. The main standards and best practices of governance were used from the perspective of cyber security in order to add new knowledge to cyber defense strategies APF. The insights gained through the topics studied in the literature review and the session management of information security in the organs of the APF showed the importance and needs of the subject matter as there is the government's own interest to be met safety requirements of information. The best governance practices reproduced by COBIT, ITIL, ISO / IEC 17799:2005 and PMBOK are a legal and regulatory framework for directing the management of information security in order to protect communications, databases and especially the APF critical infrastructure. Despite the growing threats and attempted attacks on applying best practices aligned to the goal of the organization provides to ensure the availability, integrity, confidentiality and authenticity. We notice that the constant transformations in the field of cybernetic enhancements require security measures at the same speed or greater velocity. So consider contributing to this work collaboratively to advance the Cybersecurity APF.

**Key words:** Cyber Defence. IT Governance. Information Security. COBIT. ITIL. ISO / IEC 17799:2005. PMBOK.



## LISTA DE FIGURAS

Figura 1- Logotipo Gestão da Segurança da Informação e Comunicações, marca registrada da Universidade de Brasília.....	15
Figura 2 - Onipresença da Informação nos principais Processos de Negócio (SÊMOLA, 2003) .....	23
Figura 3 - Usuários da internet no mundo (GROUP, 2012).....	26
Figura 4 – Nação Virtual.....	27
Figura 5 - Quatro momentos do ciclo de vida da informação segundo Sêmola (2003) .....	32
Figura 6 - Diversidade panorâmica das vulnerabilidades que expõem o negócio a ameaças associadas (SÊMOLA, 2003).....	35
Figura 7– Como peças que se encaixam, ameaças específicas exploram vulnerabilidades compatíveis (SÊMOLA, 2003). .....	36
Figura 8– Computadores remotos deixando uma rede aberta a ataques (CRONKHITE; MCCULLOUGH, 2001, p.108).....	38
Figura 9 – Fatores Motivadores da Governança de TI .....	48
Figura 10 – Visão geral do modelo de Governança de TI (Fernandes & Abreu, p. 41) .....	49
Figura 11 - Áreas-Foco da Governança de TI, na visão do COBIT (ITGI, 2007).....	51
Figura 12 - Domínios inter-relacionados do COBIT (ITGI, 2007). .....	52
Figura 13 - Cubo COBIT (ITGI, 2007). .....	54
Figura 14 - Posicionamento processos da ITIL (Magalhães & Pinheiro, 2007, p. 66). .....	55
Figura 15 – O Núcleo da ITIL (Fernandes & Abreu, 2012, p. 258).....	58
Figura 16 - Modelo PDCA aplicado ao SGSI (ABNT, 2006, p.v) .....	62
Figura 17 - Áreas do conhecimento do PMBOK (PMI, 2008) .....	66
Figura 18 - Relação entre os grupos de processos.....	68
Figura 19 - Indicadores de Segurança da Informação na APF.....	71
Figura 20 - Hierarquia dos principais órgãos da APF na segurança e defesa cibernética.....	72
Figura 21 - Organograma do DSIC (DSIC, 2012).....	74

Figura 22 - Ministério da Defesa - Forças Armadas .....	75
Figura 23 – Postura da Defesa Cibernética.....	78
Figura 24 - Atuação em Segurança e Defesa Cibernética .....	80
Figura 25 - A Governança de Segurança da Informação. Fonte: ITGI, 2006. ....	84
Figura 26 - Conteúdo do COBIT (ISACA, 2007).....	86
Figura 27 - Gestão da Segurança no ITIL .....	88
Figura 28– Pontos mais críticos para o negócio.....	90
Figura 29 – Processo de Gerenciamento dos Riscos; adaptado (MAGALHAES; PINHEIRO, 2007, p. 412).....	91
Figura 30 – passos para análise das vulnerabilidades.....	91

## LISTA DE TABELAS

Tabela 1 - Recursos que devem ser protegidos quanto ao acesso lógico. ....	42
Tabela 2- Modelos de maturidade.....	53
Tabela 3 – Níveis de Maturidade PCN.....	56
Tabela 4 - Publicações, processos e Orientações da ITIL. ....	59
Tabela 5 - Papéis na Segurança e Defesa Cibernética. (Mandarino Junior, 2010, p. 119).....	79
Tabela 6 - Legislações de Segurança da Informação na APF. ....	82
Tabela 7 - Objetivos da GSI .....	85
Tabela 8 – Categorias de impacto; (Fonte: MAGALHAES; PINHEIRO, 2007).....	92
Tabela 9 - Correlação da ISO 17799 com os modelos COBIT e ITIL como proposta para um modelo de Governança da Segurança da Informação (Bernardes & Moreira, 2005). ....	98
Tabela 10 - Dispositivos Legais Federais de segurança da Informação ( <a href="http://dsic.planalto.gov.br">http://dsic.planalto.gov.br</a> , 2012) .....	114
Tabela 11 - Legislação Específica Federal de Segurança da Informação ( <a href="http://dsic.planalto.gov.br">http://dsic.planalto.gov.br</a> , 2012) .....	118
Tabela 12 - Projetos de Lei de Segurança da Informação ( <a href="http://dsic.planalto.gov.br">http://dsic.planalto.gov.br</a> , 2012). ....	120
Tabela 13 - Relacionamento de Processos entre os modelos ITIL e COBIT e a norma ISO 17799 (Bernardes & Moreira, 2005).....	121

## SUMÁRIO

1. INTRODUÇÃO.....	14
1.1. Origem do Trabalho.....	16
1.2. Importância do Trabalho.....	17
1.3. Justificativa.....	18
1.4. Objetivos .....	19
1.4.1. Objetivo Geral.....	19
1.4.2. Objetivos Específicos.....	19
1.5. Limitações do Trabalho .....	20
1.6. Metodologia.....	20
1.7. Estrutura do Trabalho.....	21
2. REVISÃO BIBLIOGRÁFICA .....	22
2.1. Sociedade da Informação e do Conhecimento.....	22
2.1.1. Valorização e Dependência da Informação .....	23
2.1.2. Ética da Informação .....	24
2.2. Espaço Cibernético .....	25
2.2.1. Ativos da Informação e Infraestruturas Críticas .....	27
2.2.2. Guerra Cibernética.....	28
2.3. Segurança da Informação e Comunicações.....	30
2.3.1. Ameaças e Vulnerabilidades.....	32
2.3.2. Prevenção e Proteção contra Ataques .....	39
2.3.3. Controles de Acesso Lógico .....	41
2.3.4. Educação e Política para Segurança de Informações .....	44
2.4. Governança de Tecnologia da Informação e Comunicações .....	46
2.4.1. Modelo COBIT .....	50
2.4.2. Modelo ITIL.....	54
2.4.3. Modelos ABNT NBR ISO/IEC 17799:2005 .....	60
2.4.4. Modelo PMBOK .....	63
3. GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS DA APF.....	68

3.1. Administração Pública Federal.....	69
3.2. Órgãos estratégicos para Segurança e Defesa Cibernética.....	72
3.3. Requisitos de Segurança da Informação Cibernética.....	76
3.4. Atuação para Segurança e Defesa Cibernética .....	78
3.5. Normas, Regulamentos e Legislações .....	80
4. PROPOSTAS DE GOVERNANÇA PARA O CENÁRIO CIBERNÉTICO BRASILEIRO.....	84
4.1. Aplicabilidade do COBIT .....	85
4.2. Aplicabilidade do ITIL .....	88
4.3. Aplicabilidade da ABNT NBR ISO/IEC ISO 17799:2005 .....	92
4.4. Aplicabilidade do PMBOK .....	96
4.5. Aplicação da Norma ISO 17799 com os Modelos COBIT e ITIL .....	97
5. CONCLUSÃO .....	98
REFERÊNCIAS.....	101
ANEXO A – QUADRO DOS DISPOSITIVOS LEGAIS DE CARÁTER FEDERAL, RELACIONADOS À SEGURANÇA DA INFORMAÇÃO.....	105
ANEXO B - QUADRO DA LEGISLAÇÃO ESPECÍFICA DE CARÁTER FEDERAL RELACIONADA À SEGURANÇA DA INFORMAÇÃO .....	115
ANEXO C - ALGUNS PROJETOS DE LEI RELACIONADOS À SEGURANÇA DA INFORMAÇÃO .....	119
ANEXO D – TABELA RELACIONAMENTO ISO 17799, COBIT E ITIL .....	121
ANEXO E – FATOS RECENTES.....	122
ANEXO F – TESTE DE CONFORMIDADE COM A NORMA ISO/IEC 17799 (SÊMOLA, 2003).....	124
ANEXO G – ARTIGO .....	132

## 1. INTRODUÇÃO

O controle das informações de valor, de alguma forma, sempre foi algo buscado pelos seres humanos, mesmo inconsciente desta necessidade. Ao longo do tempo, vêm se aperfeiçoando as formas das informações serem inscritas e armazenadas (CARUSO; STEFFEN, 1999). Os avanços, após as três grandes revoluções – a agrícola, a industrial e a tecnológica –, tornaram conjunto de dados na informação o atual combustível do mundo que se materializa na sua transformação em conhecimento. Atualmente, é inimaginável sobreviver sem uso da tecnologia em maior ou menor grau, pois há cada vez mais dependência da infraestrutura digital pelos governos e indivíduos.

Nesta chamada “Era do Conhecimento”, a informação tem status estratégico devido ao uso em grande escala de tecnologia da informação por meio da conectividade proporcionada pela internet, mas a estratégia de segurança deve fazer parte naturalmente dessa rotina. O sucesso das organizações públicas ou privadas depende de ter confiável e segura sua infraestrutura de tecnologia da informação. A rede mundial de computadores converge inúmeros serviços que implicam em milhões de acessos para a realização de variadas atividades do dia a dia, compartilhando o mesmo espaço (CARVALHO, 2011).

O ambiente virtual, sem fronteiras claramente definidas, formado por Tecnologias da Informação e Comunicações (TIC) interage com o mundo real no contexto da nova sociedade da informação; é conhecido como espaço cibernético ou ciberespaço. Segundo Mandarin Junior (2010), além dos benefícios para gerenciar, desenvolver e comunicar ocorre, também, o aumento da vulnerabilidade inerente a tais tecnologias. Surge a necessidade de estar comprometido com a segurança e defesa desse espaço digital pela alta administração do Estado da mesma forma que ocorre com instalações urbanas, em atenção às características dos sistemas tecnológicos para o bem estar da sociedade da informação.

Faz-se necessária, também, uma análise da forma como é gerenciada a segurança das infraestruturas da informação pela alta administração dos órgãos da

Administração Pública Federal sob a abordagem das estratégias de governança de TI para melhorar metodologias, normas, procedimentos, diretrizes, políticas e demais ações no intuito de aprimorar a gestão da segurança da informação junto aos servidores públicos nas organizações onde atuam. Muitas dessas infraestruturas são críticas por não poderem ter interrompida sua continuidade, algo que traria consequências inmensuráveis e irreversíveis para sociedade, economia, política, e segurança nacional.

**Figura 1 - Logotipo Gestão da Segurança da Informação e Comunicações, marca registrada da Universidade de Brasília.**



Muitos ataques cibernéticos têm ocorrido no mundo, causando preocupações quanto à vulnerabilidade dos diversos setores relevantes à sociedade. Por não ser uma ciência exata, as organizações públicas devem ter uma filosofia bem definida, baseada em políticas, regulamentos e guias de boas práticas, ressaltando a importância de uma filosofia de segurança apropriadamente implementada que atue minimizando impactos possíveis no uso da informação, mediante ações coordenadas e preventivas com o envolvimento do governo federal (FONTES, 2006).

O Gabinete de Segurança Institucional da Presidência da República (GSIPR) é o órgão que possui atividade inerente de coordenar as atividades de segurança da informação, em atenção ao Estado (MANDARINO JUNIOR; CANONGIA, 2010). Ele define as infraestruturas críticas da informação a fim de coordenar as atividades de segurança para minimizar a vulnerabilidade para proteção a possíveis ataques

cibernéticos.

Aplicar a Governança de TI efetivamente para garantir a criação de valor garante ao país uma forte confiabilidade perante o cenário internacional, algo que é uma vantagem competitiva significativa. As decisões relacionadas à TI exigem participação intensa dos gestores de negócio referente aos investimentos em segurança cibernética. O destaque atribuído à TI inclui a relevância do componente humano que manipula as informações. A análise da governança exige um foco na identificação das decisões fundamentais a serem tomadas e quem está em melhor condição de tomá-las (WEILL; ROSS, 2004).

Pensando em tudo isso, metodologias de governança COBIT, ITIL, NBR ISO/IEC 17799:2005 e PMBOK são utilizadas como ferramentas para melhor analisar todo o processo de tratamento dado pela Administração Pública Federal (APF) às infraestruturas críticas da informação para a garantia de sua segurança e de que forma podem ser aperfeiçoadas.

## **1.1. Origem do Trabalho**

A informação é um ativo intangível crítico e valioso para organizações e como tal deve ser protegida nos ambientes onde são processadas, armazenadas e transmitidas independentemente de seu formato (ISO/IEC 27002, 2005). Os riscos têm a proporção do significado que representa para o patrimônio da organização. Uma prática constantemente adotada pela moderna gestão é o compartilhamento da informação para maior agilidade das ações. Ela passa a ser cada vez mais digitalizada, compartilhada e distribuída, o que eleva a dependência de toda a tecnologia que a permeia (SÊMOLA, 2003).

A administração pública brasileira visando a atender à demanda por serviços de maior qualidade amplia o uso de sistemas computadorizados para realizar ações de Gestão Pública. A energia, defesa, transporte, telecomunicações, finanças e a própria informação são infraestruturas críticas do país que preocupam quanto à segurança cibernética, colocando-a como parte da função estratégica do Estado. O grande desafio está em desenvolver a gestão da segurança cibernética para evitar ou reduzir as vulnerabilidades dos sistemas de informação da Administração Pública



Federal, algo que beneficia todos os seguimentos da sociedade.

Apenas tendo departamento ou unidade administrativa que cuide da segurança cibernética da APF pode não ser suficiente para garantir o apoio necessário às operações nas condições geográfica, populacional e territorial do país. Contudo, sugere-se que se busque um controle efetivo das etapas de gestão da segurança por meio de ferramentas de governança de TI para aperfeiçoar e formalizar processos.

A Governança está presente em toda empresa, seja ela pública ou privada, mas requer técnicas diferentes para cada aplicação. A proteção contra ataques cibernéticos requer a especialização do processo em cada área, cada uma assumindo suas responsabilidades, seja de natureza estratégica ou operacional (VIEIRA, 2007). As metodologias e ferramentas COBIT, ITIL, NBR ISO/IEC 17799:2005 e PMBOK são as escolhidas a fim de serem analisadas para aplicação nos processos de segurança cibernética, implantação, gerenciamento e controle de segurança, respectivamente.

## **1.2. Importância do Trabalho**

Segundo Mandarino (Livro Verde, 2010, p.14) ocorrem os seguintes fatores na sociedade da informação:

- elevada convergência tecnológica;
- aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos;
- aumento crescente e bastante substantivo de acesso à Internet e das redes sociais;
- avanços das tecnologias de informação e comunicações (TICs);
- aumento das ameaças e das vulnerabilidades de segurança cibernética; e,
- ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças.

O estudo sobre Governança de Segurança da Informação da APF tem importância prática para realizações de ações que viabilizem e assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações. Embora a IN nº 1 do GSIPR (2008) tenha características semelhantes a ABNT NBR

ISO/IEC 17799:2005 percebe-se que há alguns aspectos que nela não são tratados e que carecem de uma abordagem própria para as organizações governamentais sob o foco de outras metodologias de Governança, tais como: a implementação da segurança da informação; gestão da segurança da informação focada na ação humana e tecnológica; estabelecimento de modelos, conceitos e metodologias inerentes às organizações brasileiras da APF; e formulação de normas adequadas para o governo nacional.

Entende-se que a análise da forma como a segurança cibernética é administrada pela APF e contribui para uma melhor coordenação de esforços a partir de estratégias e planos para o Governo Federal com a realização de ajustes contínuos, dada a evolução constante das TICs. As práticas mais apropriadas para a TI, foco da Governança de TI, são de grande valia para alcançar maior valor para as aplicações tecnológicas do Governo.

### **1.3. Justificativa**

Segundo Vieira (2007, p.7), desde os ataques terroristas de 11 de setembro, tem havido pressão para uma maior proteção contra essa categoria de ataque. Há também os casos de escândalos corporativos de fraudes em um passado recente de nosso país, fatos que chamam atenções para os mecanismos de segurança que podem ser mais bem gerenciados dadas as tecnologias atuais. A segurança cibernética na APF pode contribuir com gerenciamento de segurança tecnológica, de modo que realizem algumas tarefas, como por exemplo, a identificação de ataques terroristas e cyberataques definindo padrões sobre “o que” e “como” deve ser feito, possibilitando alterações nas legislações e normas nacionais. O indevido uso da informação, por desconhecimento, erro ou acidente deve ser tratado com diligência e responsabilidades devidas.

A segurança da informação já foi tratada sob muitos aspectos técnicos com uso de ferramentas de hardware e software. Não se deseja realizar um trabalho pautado nesses aspectos, mas providenciando um direcionamento a respeito da segurança cibernética na APF com base em um entendimento aplicado da Governança de TI.

Recentemente foi desenvolvido o Modelo de Gestão de Segurança da Informação (MGSIC), utilizado pela APF buscando conformidade com a Governança

de TI. Todo esse trabalho vem sendo bem aproveitado e tem dado resultados, porém carece de um estudo aprofundado de métodos de governança de TI para melhor fundamentação de um modelo de segurança da cibernética na APF que esteja em conformidade com as ferramentas de Governança de TI. Este trabalho se remete a investigar a complexidade do tema por sua importância estratégica a fim de possibilitar a adequada gestão e uso seguro das infraestruturas de TI críticas do país.

## **1.4. Objetivos**

### **1.4.1. Objetivo Geral**

Analisar de forma holística e sistêmica a forma de Gestão da Segurança da Informação adotada pelo Governo por meio de ferramentas amplamente difundidas de Governança de TI, como COBIT, ITIL, NBR ISO/IEC 17799:2005 e PMBOK. Assim, sugere-se colaborar com o embasamento teórico atual para a metodologia adotada pelo Departamento de Segurança da Informação e Comunicações (DSIC), subordinado ao Gabinete de Segurança Institucional da Presidência da República (GSIPR), a fim de que sejam úteis para seus processos, alcançando melhorias no resultado.

### **1.4.2. Objetivos Específicos**

Fazer uma descrição contextualizada dos assuntos relacionados ao tema do trabalho e análise global e sistêmica de documentos publicados pelo governo sobre Segurança Cibernética, Segurança da Informação e Comunicações, Segurança das Infraestruturas Críticas da Informação, entre outros documentos oficiais. A partir disso, identificar os principais posicionamentos, procedimentos e expectativas, considerando o uso das tecnologias, recursos humanos, riscos, a política organizacional no âmbito Administração Pública Federal.

Demonstrar com as estruturas já estabelecidas de boas práticas de Governança quais são os processos passíveis de serem aplicados no planejamento estratégico de segurança da informação dos Sistemas de Informações Gerenciais da

APF.

Tratar alguns pontos específicos como, controles (o que), processos (como), pessoas (quem) e tecnologia (ferramentas automatizadas) utilizando:

- COBIT e ISO/IEC 17799 para definições de objetivos de controles;
- ITIL, para definir os processos; e
- PMBOK, para implantação da gestão da segurança. Tais práticas devem se encaixar no processo de segurança cibernética, sendo demonstrada a sua aplicabilidade.

## **1.5. Limitações do Trabalho**

A abrangência deste trabalho possibilita muitas variações. Nem todas são abordadas intencionalmente a fim de não fugir do foco em questão. Não pretende atender a questões aprofundadas de rede de computadores, especificações computacionais, segurança de dados e segurança de código, nem todas as complexidades a eles inerentes. O tema segurança da informação é abordado sob a ótica da gestão de tecnologia para que o gerenciamento dos sistemas atenda as necessidades das organizações da APF.

## **1.6. Metodologia**

Toda a análise documental realizada neste trabalho se dá por meio de pesquisa exploratória não experimental utilizando livros, artigos, e outras publicações do governo e a ele referente.

Foram escolhidos os modelos de boas práticas de gerenciamento COBIT, ITIL, PMBOK e a norma ISO/IEC 17799 por serem os que melhores se aplicam ao estudo da Segurança Cibernética na APF e para o cumprimento do objetivo geral deste trabalho.

Este material pode ser usado tanto para aprender princípios básicos de Governança de Segurança da Informação e também para servir como auxílio e pesquisa na implantação da gestão da segurança cibernética em órgão público. A validade das propostas apresentadas ocorre com fundamento na qualidade das

evidências alcançadas, por meio de análises, comparações e demonstrações teóricas.

## **1.7. Estrutura do Trabalho**

Este trabalho é composto por cinco capítulos cuja organização dos elementos textuais está disposta como se segue:

A segunda sessão corresponde à revisão bibliográfica na qual são apresentados os conceitos de autores, sempre que possível de mais de uma fonte, relacionados ao tema, servindo de referência para os tópicos posteriores. Os modelos de Governança de TICs são descritos de modo mais aprofundado e cuidadoso por se tratarem de alvos amplamente indicados em sua aplicabilidade na APF.

A terceira sessão mostra como é feita a gestão da segurança da informação na APF com base na pesquisa documental do governo, identificando os pontos chave a serem analisados com uso das ferramentas de Governança de TI.

Na quarta sessão, são feitas propostas deste trabalho aplicadas ao cenário brasileiro e o que vem sendo feito para melhorá-lo. Identifica como estabelecer a simbiose entre a segurança cibernética e o dia a dia dos órgãos da APF.

A quinta sessão, referente à conclusão, expõe os aspectos positivos e negativos do trabalho, bem como os mais relevantes do processo de desenvolvimento para se chegar aos objetivos propostos. As ocorrências de onde foram tiradas informações relevantes sobre o tema ao longo do trabalho são indicadas de modo que possam ser úteis a quem desejar utilizar o material.

## 2. REVISÃO BIBLIOGRÁFICA

### 2.1. Sociedade da Informação e do Conhecimento

Embora seja empregado para a sociedade contemporânea, o termo “Sociedade da Informação” é utilizado como consequência das análises de Peter Drucker, em seu livro *A era da descontinuidade*, em 1970, para o Produto Interno Bruto dos Estados Unidos da América. Com isso, sociedade da informação acabou sendo definida como “a etapa do desenvolvimento da sociedade que se caracteriza pela abundância de informação organizada” (OLIVEIRA et al., 2005, p.113).

Atualmente esse termo, juntamente com “globalização”, carrega a expectativa de propagação do conhecimento em todas as áreas da sociedade exercido pelo uso de tecnologias da informação e comunicações. Mandarino Junior (2009) afirma que a expressão é válida, ainda que sem uma definição comumente aceita, resultado das facilidades em adquirir soluções em tecnologia. Mandarino Júnior (2010) afirma que:

O conceito de sociedade da informação é decorrente da estratégia de reorganização econômica do pós-guerra e surgiu como fruto da acelerada industrialização experimentada nos últimos 50 anos, que estabeleceu alterações profundas na relação homem x tecnologia [...].

Ocorre que a essencialidade da informação depende de sua presença num ambiente que gere conhecimento (SORJ, 2003), pois proporciona os benefícios do uso da tecnologia da informação e comunicações.

O vocábulo “conhecimento” é definido conforme o direcionamento das áreas de estudo quando forma “sociedade do conhecimento”, quase tão difundido quanto “sociedade da informação”. Segundo Sorj (2003), torna-se mais satisfatório para ser aplicado como referência aos processos de estudos que implicam em avanço da capacidade de inovação tecnológica, base da economia atual.

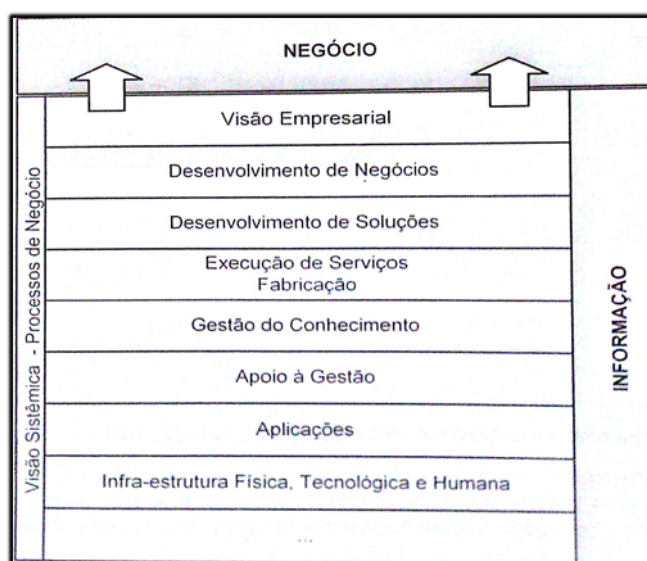
O mais relevante para fins deste estudo é que os cidadãos e as organizações sofrem transformações em virtude dos rumos dos processos que ocorrem na sociedade da Informação e do conhecimento, em muitas áreas, a exemplo do

Governo de Estado.

### 2.1.1. Valorização e Dependência da Informação

A expansão da Internet proporciona que milhares de pessoas a acessem e os efeitos da tecnologia da informação a ela associada promovam quebras de paradigma que impactam instituições, negócios e indivíduos por meio de constantes descobertas. Segundo Sêmola (2003), a informação passa ser um ativo cada vez mais valorizado, presente em diversos patamares de gestão de negócios. Weill e Ross (2004 apud BERNARDES e MOREIRA, 2005, p.1) nos passam o ponto de vista de que “a informação é reconhecida pelas organizações nos últimos anos como sendo um dos mais importantes recursos estratégicos que necessitam de gerenciamento”.

Figura 2 - Onipresença da Informação nos principais Processos de Negócio



Fonte: (SÊMOLA, 2003)

É improvável imaginar as relações de negócios hoje em dia sem o uso de sistemas de informação. A convergência tecnológica, resultado de inovações constantes, faz com que o surgimento e armazenamento das informações ocorram em pontos distintos e percorram o mundo por canais na maioria das vezes desconhecidos e livremente em um tempo insignificante. Essa infraestrutura faz com que as empresas introduzam cada vez mais aplicações comerciais para

dependentes das tecnologias, como por exemplo: “business-to-business”, “business-to-consumer”, “business-to-government”, “e-commerce”, “e-procurement”, e os sistemas ligados “ERP” (SÊMOLA, 2003).

### 2.1.2. Ética da Informação

Essa nova sociedade do conhecimento, como em qualquer outra, atraiu pessoas mal intencionadas, que buscam obter vantagens indevidas, explorando falhas nos sistemas. A vacância legislativa no trato das novas tecnologias, além do pseudo-anonimado pela ausência física do ofensor facilitaram a ação desses invasores.

Segundo Masiero (2008), o profissional da computação, para ser digno de ser acatado com apreço perante a sociedade, precisa ter um comportamento ético; caso contrário, gera vergonha para a profissão. Segundo o autor, os códigos de ética para o setor de computação ainda não estão solidificados, a exemplo de outras profissões mais antigas na sociedade.

Sobre definição de ética, Masiero (2008, p.20) afirma:

É um ramo da filosofia que estuda o comportamento moral do ser humano, classificando-o como bom ou ruim, correto ou errado. Os conceitos éticos provavelmente surgiram quando o ser humano começou a viver em sociedade e aprendeu a identificar certos comportamentos como positivos ou negativos para o bem-estar e segurança do grupo [...].

Os sistemas de informação muitas vezes colocam-se em conflito com alguns limites éticos representados por crimes digitais, que podem abranger: invasão de privacidade, espionagem empresarial, pedofilia, discriminação e furto de dados financeiros. Esterbauer, Ruckenbauer e Kolb (2001, p.57) afirmam:

[...] A tecnologia da informação está sempre à frente de juízes e legisladores. O usuário, de sua parte, está acostumado a mover-se em um espaço isento de leis. E o mais difícil é quando também faltam, nesse espaço sem lei, quaisquer indicadores de valores morais ou normas sociais [...].

Há preocupações quanto ao aumento do número de tecnologias de dispositivos móveis, redes sociais, *cloud computing* e *outsourcing*. São muitos os riscos ligados a essas tecnologias tanto para organizações quanto para o usuário comum. O termo



de compromisso registra a responsabilidade de um funcionário, deixando claro o padrão ético esperado pela organização de um profissional qualificado, mas quando são descumpridos, seja moralmente ou culturalmente, os ilícitos devem ser tratados, penalizados administrativamente e, quando mais graves, relacionados com as leis penais vigentes.

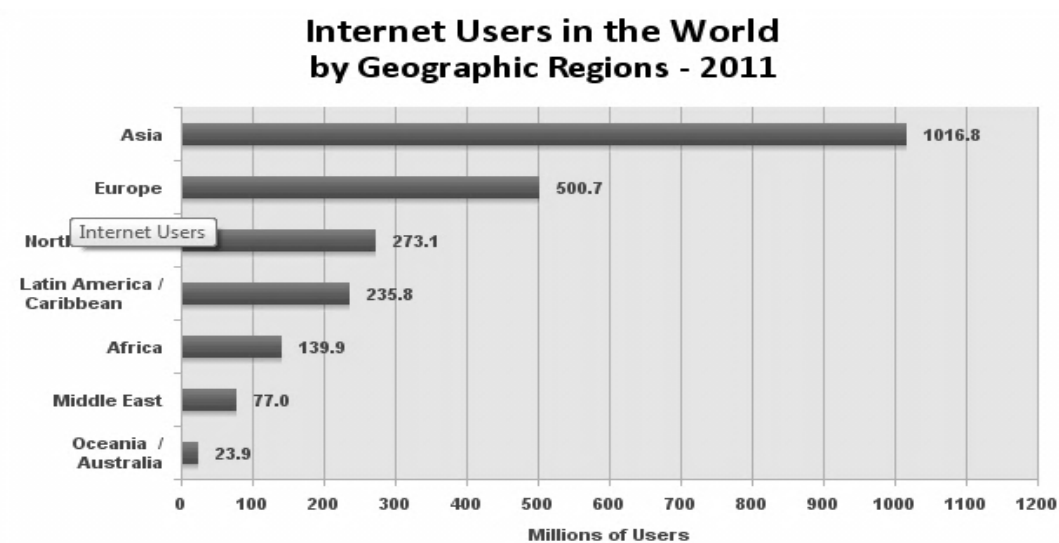
## **2.2. Espaço Cibernético**

O conceito estabelecido no I Seminário de Defesa Cibernética do Ministério da Defesa é definido como:

**Espaço Cibernético** - Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas. Ações ofensivas no espaço cibernético podem impactar, inclusive, a segurança nacional.

Cibernética relaciona o ser humano e os efeitos provocados pelas máquinas tecnológicas. Este neologismo da Era da informação configura um território desafiador por estar fora dos limites tradicionais físicos estabelecidos pelas fronteiras geopolíticas e organizacionais, revolucionado pelas novas formas de trocas de informações com percepção coletiva e constantemente modificada devido ao avanço das tecnologias. Isso faz com que surjam conflitos difíceis de serem resolvidos, cabendo intervenção do poder público ativamente nesse novo espaço (CARVALHO, 2011). As complexas redes de interconexão autorreguladas e autônomas muitas vezes são utilizadas inconseqüentemente para acessos a infraestruturas críticas sem o conhecimento técnico necessário.

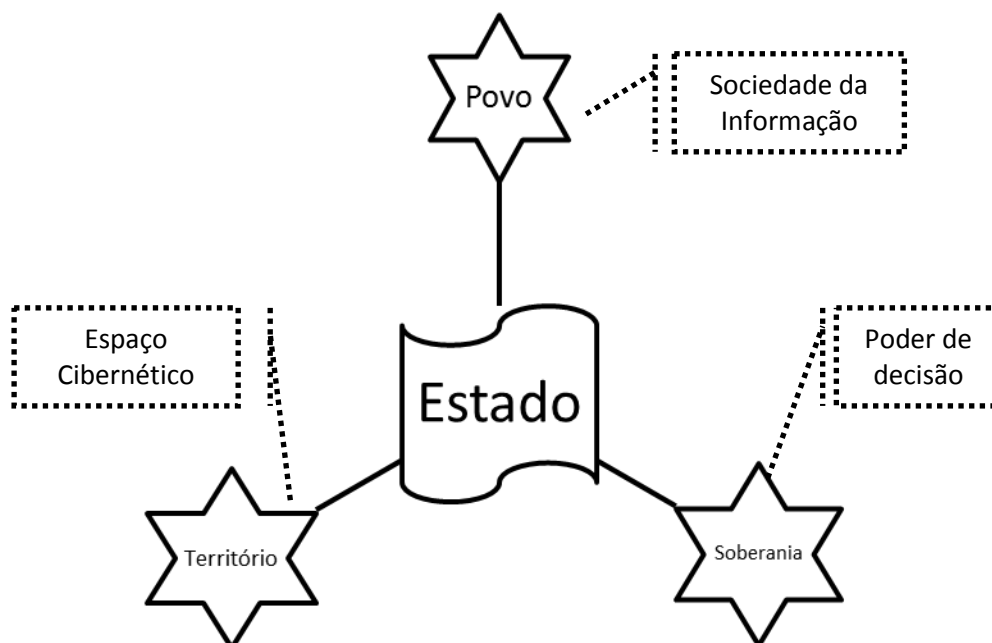
Figura 3 - Usuários da Internet no mundo.



Fonte: (GROUP, 2012).

A presença de elementos constituintes da formação de um Estado estabelece o que pode ser chamado de “nação virtual”, algo que exige estratégias de proteção e defesa em sua estrutura. Os elementos são os seguintes (MANDARINO, 2010, p.41): “Povo, caracterizado pela sociedade da informação. Território, pelo próprio espaço cibernético. Soberania, a capacidade de controlar, de ter poder de decisão sobre o espaço”.

Figura 4 – Nação Virtual



### 2.2.1. Ativos da Informação e Infraestruturas Críticas

De acordo com o Guia de Segurança das Infraestruturas Críticas da Informação da Presidência da República (2010), as infraestruturas críticas da informação pertencem aos chamados ativos da informação. Estes tratam de armazenar, transmitir e processar os sistemas de informação, bem como os locais onde se encontram e os seus usuários. Confunde-se em sua definição com a própria sociedade da informação.

As organizações públicas devem satisfação à população na forma de serviços prestados proporcionando-lhes melhores condições. O governo investe recursos de forma que a continuidade permaneça e as contingências e desastres sejam administrados para não comprometer esses serviços. Para situação com pouca probabilidade de ocorrência, Fontes (2006, p.62) informa que a pergunta correta a ser feita diante dela é “E se isso acontecer?”.

As infraestruturas da informação são definidas como críticas porque a interrupção do funcionamento de hardware, software ou serviços acarretaria um enorme impacto social, econômico, político, internacional ou de segurança nacional

(BRASIL, 2008), assim como os casos advindos de causas naturais.

Seguem abaixo alguns exemplos de infraestruturas críticas normalmente de responsabilidade da APF que podem ser alvos de guerra cibernética:

- Setor energético;
- Setor financeiro e bancário;
- Setor de transportes;
- Setor de telecomunicações;
- Fornecimento de água;
- Rede hospitalar;
- Órgãos de defesa e segurança pública;
- Polos tecnológicos.

Ataques sofridos nos ambientes acima apresentados causam impacto elevado nos interesses nacionais e ferem a soberania do Estado. Devido ao fato de o ciberespaço e o mundo físico estarem cada vez mais ligados pelas tecnologias pode-se concluir que garantir a soberania de uma nação também significa garantir a soberania de sua atuação dentro do espaço cibernético.

### **2.2.2. Guerra Cibernética**

Tão importante quanto defender instalações urbanas é a proteção do espaço cibernético. Ataques com armas de guerra podem causar tanto impacto quanto ataques virtuais. São muitos os problemas capazes de causar mortes, a título de exemplo: apagão elétrico, descontrole de sistemas de tráfego aéreo ou de trens. Para muitos terroristas ou “ciberterroristas” explorar essas novas armas podem dar o alcance necessário para realizarem seus ataques. É um novo domínio de guerra, a “ciberguerra”, tanto quanto, mar, terra, ar e o espaço.

Em muitos casos o Estado deve agir para identificação e combate a ações criminosas de terrorismo e sabotagem na guerra cibernética, nessa que é a área de atuação militar de defesa cibernética.

Uma definição feita pelo Ministério da Defesa (2008) para este tipo de guerra:

Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens

tanto na área militar quanto na área civil.

Guerra cibernética tem necessariamente as seguintes características segundo Branco Júnior (2005):

- é ramo da guerra da informação;
- refere-se a ações militares estratégicas, operacionais e táticas, realizadas no ciberespaço;
- emprega meios de tecnologia da informação (comunicações, computação e informática);
- possui dois objetivos: explorar as infraestruturas e sistemas de tecnologia de informação do adversário e obter a supremacia da informação ou ao uso da informação para obter vantagem sobre o adversário;
- um dos atores envolvido é um Estado Soberano ou um de seus órgãos de defesa, não importando quais sejam os demais atores envolvidos, nem as suas motivações;
- empregada em tempos de paz ou de crise (conflito).

A taxonomia para guerra cibernética é composta por sete fatores que atuam combinadamente, os quais são apresentados abaixo (LIBICKI, 1995):

- *command-and-control warfare* (C2W) ou guerra de comando e controle;
- *intelligence-based warfare* (IBW) ou guerra baseada na inteligência;
- *electronic warfare* (EW) ou guerra eletrônica;
- *psychological operations* (PSYOPS) ou operações psicológicas;
- *hackerwar* ou guerra de hacker;
- *economic information warfare* (EIW) ou guerra de informações econômicas;
- *cyberwar*(CW) ou guerra cibernética.

A segurança e defesa cibernética são amplamente debatidas atualmente e é uma tendência mundial, considerando a urgência de muitas indefinições sobre o assunto, uma vez que estão ligadas à prestação de serviços para a qual a sociedade depende em diversos sentidos. Trata-se de um novo domínio de guerra, dentro da gestão de política nacional, pela sua absoluta relevância e suas características

próprias. São muitas as ameaças para derrubar os pilares da integridade, autenticidade, disponibilidade e confidencialidade dos sistemas cibernéticos (CARVALHO, 2011).

Ribeiro (2011) afirma ser de enorme importância que haja monitoramento e realização de teatro de operações para alcançar a eficiência na proteção do espaço cibernético e, assim, garantir a utilização das redes de comunicações e de computadores.

### 2.3. Segurança da Informação e Comunicações

A informação é um bem que deve ser gerenciado adequadamente para garantia de sucesso do negócio da organização. A Instrução Normativa 001/GSI, de 13 de junho de 2008, disciplina a Gestão da Segurança da Informação e Comunicações e estabelece conceitos em seu artigo 2º dentre os quais os abaixo listados:

- **Segurança Informação e Comunicações** - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
- **Disponibilidade** – a informação disponível para os usuários fazerem uso quando delas necessitarem.
- **Integridade** – a informação preservada após a disponibilização pelo proprietário a fim de que não seja alterada sem seu consentimento.
- **Confidencialidade** – a informação protegida conforme classificação do seu conteúdo para restrição do acesso a pessoas autorizadas.
- **Autenticidade** – a informação identificada formalmente quanto à procedência, ao remetente, à alteração e ao recebimento.
- **Gestão de Segurança da Informação e Comunicações** - ações e métodos para a integração do exercício de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

Os riscos de segurança da informação associados ao funcionamento de uma organização pública podem dificultar ou impossibilitar o funcionamento da infraestrutura de um serviço relevante prestado ao país. O valor desses serviços prestados pela organização deve ser avaliado e conhecido de acordo com os riscos de ocorrer uma perda da continuidade do desempenho do negócio.

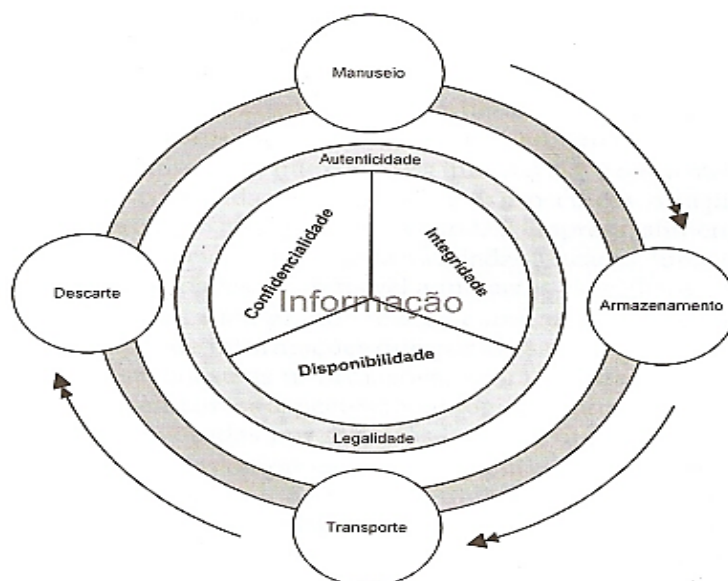
Um ditado popular foi citado por Caruso e Steffen (1999, p.21) que diz: “nenhuma corrente é mais forte que seu elo mais fraco”. De tal modo, a gestão da segurança da informação objetiva preservar as informações eliminando as vulnerabilidades e garantindo o máximo de benefícios do sistema.

A Associação Brasileira de Normas Técnicas – ABNT NBR/ISO/IEC 27002:2005 prevê os seguintes conceitos:

A **informação** [grifo meu] é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente [sic] necessita ser adequadamente protegida. [...] A **segurança da informação** [grifo meu] 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 necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Algumas circunstâncias estão associadas à proteção da informação, como acesso físico e lógico, propriedade, custódia, controle de acesso, plano de contingência, e preservação e recuperação de informações. Tudo isso deve ocorrer durante todo o ciclo de vida da informação. Esse período pode ser dividido nas ocasiões: manuseio, armazenamento, transporte e descarte (SÊMOLA, 2003).

Figura 5. Quatro momentos do ciclo de vida da informação.



Fonte: Sêmola (2003).

A expressão “comunicações” refere-se ao processo de transmitir e reproduzir parte do tratamento dado à informação de forma segura e correta para o exercício do poder das organizações governamentais ao qual está submetida.

Existem algumas ideias equivocadas a respeito da segurança exemplificadas por Caruso e Steffen (1999), que merecem ser mencionadas:

- “UMA vez implantada a segurança, as informações estão seguras.”
- “A implantação da segurança é um processo simples.”
- “A segurança é um assunto de exclusiva responsabilidade da área de segurança.”
- “A estrutura de segurança é relativamente estática.”

### 2.3.1. Ameaças e Vulnerabilidades

Ferrari, Cornachine e Loyola (2011) em matéria de capa da revista Época traz o seguinte texto: “Os ataques a sites oficiais brasileiros dão o alerta para luta entre nações e organizações na Internet. E revelam como estamos vulneráveis”. Tal assunto chama bastante atenção e nos indaga: será que estamos realmente vulneráveis e como podemos resolver isso?

O usuário, no exercício de sua tarefa rotineira, estando conectado a uma rede de troca de dados está vulnerável a ataques cibernéticos por mais seguro que possa



estar este ambiente. Não existe um sistema completamente seguro e isento de ataques, exceto se livre de interconexão, algo raro de ocorrer. As ameaças e ataques podem ser de natureza física ou lógica. As ameaças internas não pertencem ao escopo deste trabalho por não se enquadrarem nos conceitos de espaço cibernético. As ameaças lógicas buscam explorar as vulnerabilidades de um sistema cibernético sendo assim tratado com relevância.

Sobre ameaças no espaço cibernético, Mitnick, considerado o hacker mais famoso da atualidade, escreveu em seu livro “A arte de Invadir” (2005, p.37):

Nossos inimigos podem muito bem estar treinando seus soldados na arte da guerra cibernética para atacar nossa infra-estrutura e defender a deles. Parece uma bobagem pensar que esses grupos também recrutariam hackers de qualquer lugar do mundo para projetos de treinamento e missões perigosas. [...] De acordo com um relato publicado no Washington Times sobre esses primeiros esforços, “Autoridades do Pentágono ficaram assustadas com um exercício militar que mostrava como é fácil para os hackers suprimir funções de redes de computador civis e militares dos Estados Unidos”. O artigo explica ainda que a National Security Agency reuniu um grupo de especialistas em computadores como uma ‘equipe vermelha’ de hackers que pudesse usar apenas equipamentos de computador, disponíveis ao público e qualquer ferramenta de hacking, inclusive explorar códigos, para fazer download da Internet ou de boletins eletrônicos.

Em alguns dias, a equipe vermelha de hackers infiltrou-se em partes de controle de sistemas de computador da rede de energia elétrica federal e com uma série de comandos deixou partes do país no escuro. “Se o exercício tivesse sido real”, de acordo com o Christian Science Monitor, “eles poderiam ter estragado os sistemas de comunicação do Departamento de Defesa (tirando a maior parte do Comando Pacífico) e ter tido acesso a sistemas de computador em embarcações da Marinha norte-americana”. [...] Há registros de que membros da Al Qaeda e outros grupos terroristas costumam usar redes de computador em atos de planejamento terrorista. As evidências sugerem que os terroristas usaram a internet para planejar suas operações para os ataques 11 de setembro.

[...] Para jovens hackers, a segurança fraca continua sendo um convite. [...] A boa segurança nunca foi tão importante em um mundo habitado por terroristas.

Segundo Cronkhite e Mccullough (2001), são algumas das possíveis motivações para um ataque cibernético:

- **Status** - A mídia dá destaque para ataques cibernéticos bem sucedidos, algo que implica em reconhecimento das habilidades do ofensor. Desta forma, sites do governo e de grandes organizações tornam-se alvos em evidência.
- **Financeiros** - Criminosos cibernéticos também se sentem atraídos por

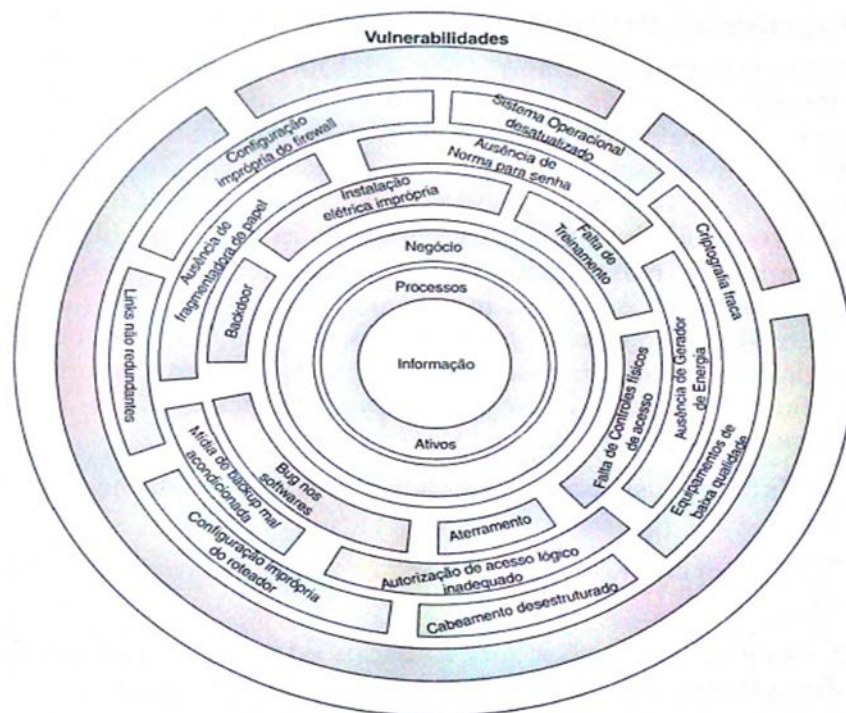
questões financeiras. Alguns alimentam o desejo de aumentar a riqueza roubando de empresas ricas, seja para uma boa causa (Robin Hood), ou para o próprio benefício.

- **Espionagem** - Segredos comerciais, militares, ou propriedade intelectual motivam outros ataques para espionagem corporativa ou governamental. Desta forma, podem fazer chantagem, usar para benefício próprio ou vender para terceiros que estejam interessados.
- **Políticos** – cada vez mais comum hoje em dia tendo como causa temas polêmicos, como por exemplo, engenharia genética, meio ambiente ou experimentos médicos. Querem chamar a atenção para a causa a que se propõem.
- **Vingança Pessoal** – causa de grande preocupação para empresas quando funcionários antigos de organizações decidem agir inadvertidamente para arruinar sistemas, destruir informações ou qualquer agressão, usando como ferramenta os conhecimentos internos ao ambiente.

Segundo a ISO 27002 (2005), ameaça é “causa potencial de um incidente indesejado, que pode resultar em um dano para o sistema ou organização”; e vulnerabilidade é “fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças”.

Se a organização possui instrução normativa de segurança incompleta ou não a possui, pouco pode fazer para identificar as ameaças e vulnerabilidades.

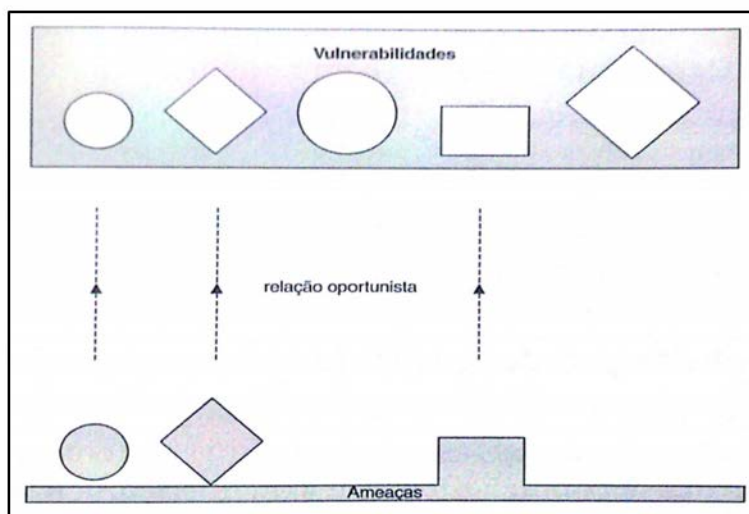
Figura 6 - Diversidade panorâmica das vulnerabilidades que expõem o negócio a ameaças associadas.



Fonte: (SÊMOLA, 2003)

A vulnerabilidade expõe aspectos tecnológicos e humanos com brechas oportunistas que podem transformar ameaças em ataques de quebra de segurança. As organizações devem ter procedimentos para descobrir, avaliar e atenuar as vulnerabilidades de segurança, cujo conhecimento faz com que seja o principal método de invasões ao sistema (ANÔNIMO, 2001).

Figura 7 – Como peças que se encaixam, ameaças específicas exploram vulnerabilidades compatíveis.



Fonte: (SÊMOLA, 2003).

Recomenda-se agrupar vulnerabilidades possíveis às quais a organização pode estar submetida, assim como as apresentadas, a fim de garantir soluções específicas para cada uma delas. Exemplificando:

#### Bugs de Software

Comportamentos imprevistos ou imprevisíveis como consequência de erros de programação, causados algumas vezes por pressa no desenvolvimento, quando não são realizados todos os testes necessários antes da sua entrega. Há situações que problemas de segurança são insuficientes para impedir um novo software de ser colocado no mercado.

#### Problemas de Configurações do Sistema

Um sistema inapropriadamente configurado que abre brechas para que o mesmo seja explorado por meio de dispositivos de rede por um acesso indevido. Ambientes computacionais sendo operados sem aplicações de *patches* ou correções de *software*. As configurações *default* por vezes são desprotegidas ou protegidas com padrões conhecidos para facilitar o trabalho de usuários inexperientes, comprometendo a segurança. Há ferramentas que exploram a rede em busca de vulnerabilidades como estas.

Programas que podem ser usados com níveis de segurança e que permitem

vulnerabilidade, deixando programa ou servidor desprotegido quanto a acessos remotos e ativação de comandos não autorizados.

### Atitudes Negligentes

Pessoas mal intencionadas costumam explorar atitudes descuidadas. Deixar serviços em execução abertamente quando na ausência representa uma atitude muito comum de usuários e, até mesmo, de administradores de sistemas. Ganho de tempo em troca de segurança pode ser um mau negócio.

O compartilhamento de recursos computacionais com base na confiança implica em vulnerabilidade quando um dos computadores tem a sua segurança comprometida e permite que todos os computadores possam ser atacados por intermédio dele, comprometendo a rede inteira.

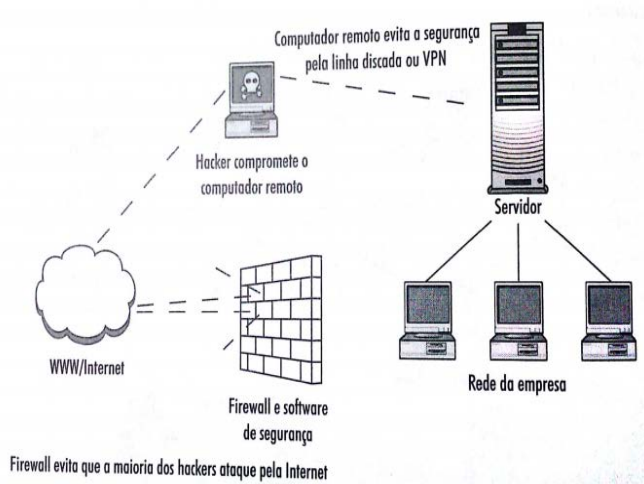
### Senhas Fracas

Algo feito para garantir a segurança quando usado incorretamente pode ser a mais fácil porta de entrada para sistemas inteiros. Existem várias maneiras de descobrir senhas quando não é dada a devida atenção a elas.

### Computadores Remotos desprotegidos

Computadores domésticos, portáteis ou móveis usados para acesso à rede corporativa por alguém mal intencionado que acesse a rede ainda que com uso de rede privada virtual (VPN), firewall ou outro dispositivo de segurança.

**Figura 8 – Computadores remotos deixando uma rede aberta a ataques.**



Fonte: (CRONKHITE; MCCULLOUGH, 2001, p.108)

### Falta de funcionários e funcionários desqualificados

As vulnerabilidades dos sistemas cibernéticos exigem um conhecimento técnico especializado e habilidades de gerentes, executivos e proprietários para que seja reduzido o menor risco possível de invasão. Alguns operadores de sistemas organizacionais não possuem experiência suficiente quando se trata de segurança cibernética, somente esse simples fato já seria preocupação suficiente, ainda que não houvesse sistemas falhos, erradas configurações e equívocos de programação. Até mesmo as organizações públicas podem carecer de profissionais de segurança.

Treinamentos na área de segurança mesmo sendo muito importantes nem sempre são viáveis devido à grande quantidade de etapas requeridas para formar um bom especialista. Além do que, pode existir outro problema para o uso incorreto de programas de segurança da informação que muitas vezes ocorre, que é a falta de pessoal.

### Sistema Operacional

Cada Sistema operacional apresenta qualidades positivas e negativas com relação à segurança. Não é difícil encontrar sistemas operacionais distintos em uma mesma rede corporativa. É preciso estar atento às características técnicas de cada um para não deixar o sistema vulnerável.

### **2.3.2. Prevenção e Proteção contra Ataques**

Esta parte do trabalho apresenta uma visão geral sobre prevenção e proteção contra ataques cibernéticos na esfera pública federal privilegiando as estruturas e processos existentes de modo que seja útil para a APF na consolidação de um sistema de segurança e defesa cibernética nacional.

Prevenção é um item extremamente relevante para proteção da infraestrutura crítica da informação. Seu principal objetivo é reduzir o número de vulnerabilidades de segurança da informação. Medidas preventivas podem ser definidas como ações que objetivam evitar que investidas ofensivas sejam danosas em grandes proporções. Pelo fato de serem variadas, independentes e complexas é utópico esperar que se esteja totalmente imune aos ataques cibernéticos. Para isso, a organização gerencia e aplica métodos de gestão de risco e põe em prática planos de contingência e de continuidade para que eventuais falhas sejam de curta duração e que os serviços sejam facilmente reestabelecido após interrupções. O importante é que os órgãos públicos estejam preparados para lidar com ataques cibernéticos em suas infraestruturas críticas da informação.

A adoção de medidas de segurança cibernética é complexa, pois envolve interesses públicos e governamentais de características variadas. É possível que se encontre nas organizações pessoas relutante em investir na gestão da segurança da informação. Muitas só se dão conta de sua real necessidade diante de um dano consumado. Nesse caso a quebra de confiança diante dos clientes do sistema já foi efetivada, sendo tarde demais para restabelecê-la. Os benefícios advindos do labor de funcionários ficam comprometidos diante de um problema imprevisto em que nem mesmo procedimentos preventivos seriam possíveis de serem eliminados. Diversos estudos nesta área são importantes para superar interesses pessoais e institucionais em prol do interesse coletivo e, mais importante que isso, para os interesses nacionais.

Partindo-se da premissa de que o tema requer primeiramente um entendimento de conceitos dinâmicos e que envolve áreas interdependentes e, em muitos casos, sobrepostas, muitos esforços devem ser coordenados no nível nacional referente ao setor cibernético. Tais esforços serão desenvolvidos ao longo deste trabalho para ajudar na consolidação e organização do sistema de segurança e defesa

cibernética.

Cumprindo o que é estabelecido na Estratégia Nacional de Defesa ações são realizadas no espaço cibernético pelas forças armadas e órgãos e entidades públicas com atividades específicas de defesa e proteção nesse ambiente. Como por exemplo:

- **Ações de inteligência** - essencial na busca de informações, empregando todas as fontes disponíveis, para identificar e prevenir ameaças cibernéticas e proporcionar respostas adequadas e oportunas.

- **Ações de Segurança Cibernética** – envolve a proteção das redes de comunicações e de computação de sua estrutura interna, bem como da interação entre os órgãos, visando colaborar efetivamente com o esforço de proteção das infraestruturas críticas nacionais.

- **Ações de Defesa Cibernética** – envolve ações defensivas e de resposta ativa, mormente nas situações de crise, estendendo-se ao uso mais abrangente de ações ofensivas nas atividades de guerra cibernética, a qual se relaciona com guerra eletrônica.

O relevante em nível de instituição pública de modo geral é que se tenha um plano baseado na razoabilidade diante de problemas de segurança que possam ocorrer em uma organização, pois por vezes a teoria não condiz com a prática a ser aplicada. De acordo como Anônimo (2001, p.30), as seguintes ações preventivas de segurança que podem ser aplicadas:

- entender onde os ativos da organização residem;
- reduzir o número de pontos de vulnerabilidade e exposição;
- tornar sistemas seguros e equipamento de infraestrutura;
- desenvolver, instalar e impor diretivas de segurança;
- desenvolver, distribuir e impor configuração padronizada de sistemas operacionais e documentos de segurança;
- treinar administradores, gerentes e desenvolvedores em áreas relevantes na segurança de informações;
- Implementar programa de resposta a incidentes;
- implementar esforço de identificação de ameaças;
- implementar mecanismo de auto-auditoria;
- educar.



Os pontos acima destacados devem ser aprofundados em trabalho oportuno considerando que a dependência de sistemas de informações conectados por uma rede de comunicação, como a internet, para a viabilização dos negócios na esfera pública.

A prevenção tem por objetivo reduzir o número de brechas de segurança da informação e evitar que algum imprevisto física ou logicamente aconteça a sistemas compostos por equipamentos; sistemas de comunicação e *softwares*. Isso pode ser alcançado através de medidas simples ou complexas. É relativamente comum organizações utilizarem barreiras computacionais e físicas para proteger suas bases de dados. Em diversas situações o funcionário, seja ele técnico ou usuário, deve estar treinado e devidamente orientado para possíveis ataques, inclusive os de engenharia social, para não fornecer informações indevidas. No entanto por as ameaças serem múltiplas, interdependentes e complexas, é utópico pensar em uma proteção 100% efetiva. Haja vista é necessário que os gestores da infraestrutura crítica da informação estejam preparados para lidar com incidentes.

Atividades de contra-ataque a ofensivas virtuais e medidas de proteção que visam a assegurar a segurança das informações, são exemplos de boas práticas: uso de antivírus, termo de compromisso, autenticação de usuário, *backup* de segurança, uso adequado de correio eletrônico e Internet, entre outros.

No ambiente estratégico do Estado, o combate a essa ameaça deve fazer parte de suas prioridades, a fim de prevenir danos à sociedade e ao próprio Estado, os quais podem assumir proporções consideráveis.

### **2.3.3. Controles de Acesso Lógico**

No uso da tecnologia para geração, armazenamento e divulgação de informações há a necessidade de um controle de acesso lógico para que as mesmas sejam mantidas livres de perdas, modificação ou divulgação, mesmo quando não seja permitido. Para isso são apresentados alguns conceitos fundamentais relacionados com a implantação desses controles por parte das organizações.

A proteção dos equipamentos de TI não se limita apenas à segurança física, mas se complementa com procedimentos e medidas para proteção dos dados, programas e sistemas contra tentativa de acessos indevidos; são os controles de

acesso lógico (CARUSO et al., 1999).

O controle de acesso lógico é relevante para a segurança da informação porque atua na identificação e autenticação de usuários; alocação, gerência e monitoramento de privilégios; limitação, monitoramento e desabilitação de acessos e prevenção de acessos não autorizados. Dessa forma garante que:

- Apenas usuários autorizados tenham acesso aos recursos;
- Os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas tarefas;
- O acesso a recursos críticos seja bem monitorado e restrito a poucas pessoas;
- Os usuários estejam impedidos de executar transações incompatíveis com sua função ou além de suas responsabilidades.

A implantação de controle de acesso lógico parte de duas premissas: qual a tecnologia objeto da proteção e a quem serão permitidos privilégios e acessos a essa tecnologia (TCU, 2008).

Abaixo, na Tabela 1, algumas tecnologias são apresentadas juntamente com a razão pela qual se justifica a proteção quanto ao acesso lógico.

**Tabela 1 - Recursos que devem ser protegidos quanto ao acesso lógico.**

<b>Tecnologia</b>	<b>Justificativa</b>
<b>Aplicativos</b>	O acesso não autorizado ao código fonte dos aplicativos pode ser usado para alterar suas funções e a lógica do programa. Por exemplo, em um aplicativo bancário, pode-se zerar os centavos de todas as contas-correntes e transferir o total dos centavos para uma determinada conta, beneficiando ilegalmente esse correntista.
<b>Arquivos de Dados</b>	Bases de dados, arquivos ou transações de bancos de dados devem ser protegidos para evitar que os dados sejam apagados ou alterados sem autorização, como, por exemplo, arquivos com a configuração do sistema, dados da folha de pagamento, dados estratégicos da empresa.
<b>Utilitários e Sistema Operacional</b>	O acesso a utilitários, como editores, compiladores, softwares de manutenção, monitoração e diagnóstico deve ser restrito, já que essas ferramentas podem ser usadas para alterar aplicativos, arquivos de dados e de configuração do sistema operacional, por exemplo. O sistema operacional é sempre um alvo bastante visado, pois sua configuração é o ponto-chave de todo o esquema de segurança. A fragilidade do sistema operacional compromete a segurança de todo o conjunto de aplicativos, utilitários e arquivos.

Tecnologia	Justificativa
<b>Arquivos de Senha</b>	A falta de proteção adequada aos arquivos que armazenam as senhas pode comprometer todo o sistema, pois uma pessoa não autorizada, ao obter identificador (ID) e senha de um usuário privilegiado, pode, intencionalmente, causar danos ao sistema. Essa pessoa dificilmente será barrada por qualquer controle de segurança instalado, já que se faz passar por um usuário autorizado.
<b>Arquivos de Log</b>	Os arquivos de log são usados para registrar ações dos usuários, constituindo-se em ótimas fontes de informação para auditorias futuras. Os logs registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram efetuadas. Um invasor ou usuário não autorizado pode tentar acessar o sistema, apagar ou alterar dados, acessar aplicativos, alterar a configuração do sistema operacional para facilitar futuras invasões, e depois alterar os arquivos de log para que suas ações não possam ser identificadas. Dessa forma, o administrador do sistema não ficará sabendo que houve uma invasão.

Para acesso a um sistema, normalmente a identificação e autenticação do usuário são realizadas por meio de identificador de usuário (ID) e senha em um processo conhecido como *logon*. São as comprovações que a tecnologia requer para garantir que o próprio usuário está com intenção de manipular o sistema. De acordo com as boas práticas de segurança do TCU (2008), o processo de *logon* eficiente além de divulgar o mínimo de informações sobre o sistema e não fornecer informações detalhadas sobre ele, deve:

- Informar que o computador só deva ser acessado por pessoas autorizadas;
- Evitar identificar o sistema ou suas aplicações até que o processo de *logon* esteja completamente concluído;
- Durante o processo de *logon*, evitar o fornecimento de mensagens de ajuda que poderiam auxiliar um usuário não autorizado a completar esse procedimento;
- Validar a informação de *logon* apenas quando todos os dados de entrada estiverem completos. Caso ocorra algum erro, o sistema não deve indicar qual parte do dado de entrada está correta ou incorreta, como, por exemplo, ID ou senha;
- Limitar o número de tentativas de *logon* sem sucesso (é recomendado um máximo de três tentativas), e ainda:

- Registrar as tentativas de acesso inválidas;
- Forçar um tempo de espera antes de permitir novas tentativas de entrada no sistema ou rejeitar qualquer tentativa posterior de acesso sem autorização específica;
- Encerrar as conexões com o computador.
- Limitar o tempo máximo para o procedimento de *logon*. Se excedido, o sistema deverá encerrar o procedimento;
- Mostrar as seguintes informações, quando o procedimento de *logon* no sistema finalizar com êxito:
  - Data e hora do último *logon* com sucesso;
  - Detalhes de qualquer tentativa de *logon* sem sucesso, desde o último procedimento realizado com sucesso.

É importante lembrar que além das senhas existem outras formas de autenticação de usuário, como *tokens*, cartões com *chip* ou tarja magnética, ou ainda sistemas biométricos. A escolha, concessão e uso da senha devem ser realizados de forma cuidadosa por parte da organização. Os usuários devem ser orientados a seguir política e regimentos da organização estando ciente das suas responsabilidades para a segurança da informação.

As regras de controle de acesso lógico são definidas em um documento da política da organização. A responsabilidade sobre esses controles são do gerente de ambiente operacional e dos proprietários dos aplicativos. O primeiro controla o acesso à rede, ao sistema operacional e ainda aos aplicativos e arquivos de dados, ou seja, protege contra invasores ou funcionários não autorizados. O segundo identifica quem pode acessar cada um dos sistemas as operações as quais poderá executar. São eles quem definem o privilégio de acesso dentro das particularidades de cada usuário (TCU, 2008).

#### **2.3.4. Educação e Política para Segurança de Informações**

Os especialistas em segurança tradicionalmente tendem a gozar de um prestígio maior, ou pelo menos sentem-se desse modo, por dominar conhecimento e administrar recursos que não estão disponíveis à maioria dos funcionários de uma organização. Em muitos casos isso gera a sensação de ser insubstituível e

consequentemente o egoísmo em passar para outros funcionários informações sobre segurança. Atualmente tal comportamento é completamente inadequado, os funcionários devem estar habilitados a agir fazendo uso de tais conhecimentos (ANÔNIMO, 2001).

Educação em segurança se torna importante para alguns e imprescindível para outros funcionários da organização, dependendo de aprofundamento de acordo com a posição ocupada. A Internet põe em risco a segurança de uma instituição e pode gerar consequências inimagináveis. Mesmo sabendo dos variados riscos, muitos se aventuram a fazer operações achando que estão seguros, quando na verdade não estão. Temos como exemplo a comunicação em texto plano, ou seja, não criptografada, que é totalmente passível de ser lida por pessoas indesejadas e muitos ignoram esse fato. Adotam o pensamento infundado de que segurança é problema só do pessoal da segurança. Infelizmente, havendo uma vulnerabilidade e todo o sistema poderá ficar comprometido. Para ajudar a mudar essa cultura, os procedimentos abaixo podem ser adotados:

- distribuição das diretivas de segurança a todos os funcionários;
- campanha de conscientização de segurança da informação;
- publicação de memorandos por executivos para organização salientando a importância de práticas significativas de segurança;
- matrizes de responsabilidades específicas de segurança na organização com apoio da alta gerência.

O zelo pela segurança das informações tende a aumentar, quando os funcionários têm consciência do seu valor para a organização, podendo até mesmo ser considerado como recurso crítico para continuidade dos serviços prestados.

Para indicar o comportamento dos funcionários no que se refere à segurança da informação, é estabelecido um conjunto de princípios e diretrizes conhecido como Política de Segurança de Informações - PSI. Esse conjunto de instruções é normalmente documentado pela área de segurança de informações, a qual também é responsável pela coordenação de sua implantação, sua aprovação e revisão. A alta administração, diversos gerentes e proprietários também participam do processo de elaboração da PSI, sendo recomendável que o maior cargo da organização seja o responsável pela sua aprovação (MONTEIRO, 2009).

A PSI deve ser consolidada em um documento com uma abordagem simples e

de fácil entendimento para que todos da organização tenham uma correta compreensão. Segundo Ferreira (2003, apud Monteiro, 2009) a PSI deve ser:

- simples;
- compreensível, ou seja, escrita de maneira clara e objetiva;
- homologada e assinada pela Alta Administração;
- estruturada, estabelecendo padrões;
- alinhada com a estratégia da missão da organização;
- orientada aos riscos, ou seja, direcionada para os riscos da organização;
- flexível, ou seja, moldável aos novos requerimentos de tecnologia;
- protetora dos ativos de informação, priorizando os de maior valor e de maior importância;
- positiva e não apenas concentrada em ações proibitivas ou punitivas;
- deve conter atribuições de regras e responsabilidades;
- deve conter a forma de educar os usuários;
- deve ser dinâmica, ser atualizada sempre que necessário;
- deve ser acessível a todos;
- deve ser exequível, ou seja, descrever as regras de comportamentos que possam ser cumpridas, fáceis de executar, tanto na área tecnológica como na humana.

A própria PSI deve prever o que deve ser feito para os casos em que não forem cumpridos seus preceitos, de acordo com sua severidade, amplitude e tipo de infrator. A punição pode ser uma mera advertência verbal ou escrita; ou, até mesmo, ação judicial (TCU, 2008).

## **2.4. Governança de Tecnologia da Informação e Comunicações**

A Governança de TI se relaciona com decisões e atribuições de responsabilidades ligadas ao uso de TI e sua administração. Seu modelo estabelece a estratégia dessa administração de acordo com os requisitos para atender aos objetivos de negócio da organização (ALBERTIN; ALBERTIN, 2010).

De acordo com o IT Governance Institute (2007, p. 7):

A governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as

estratégias da organização.

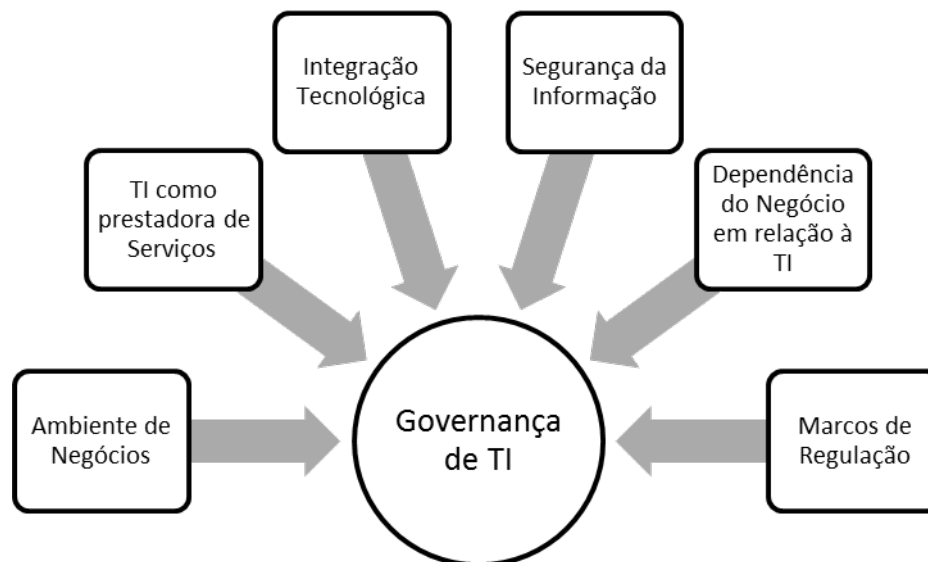
Há também outra definição dada que auxilia a conceituação de Governança de TI (WEILL; ROSS, 2004):

Governança de TI: a especificação dos direitos de decisão e responsabilidade, visando a encorajar comportamentos desejáveis no uso da TI.

Pode-se concluir partindo dessas definições que não se trata apenas de estabelecer os modelos de melhores práticas; busca-se o alinhamento da TI como a área para a qual a tecnologia será desenvolvida. Ela deve garantir a continuidade do negócio contra qualquer fato que possa comprometer o correto funcionamento, tendo que, para isso, monitorar e gerenciar as aplicações e infraestruturas de serviços.

São vários os fatores que fundamentam a implantação da Governança de TI (FERNANDES; ABREU, 2008), como demonstrados na Figura 9:

**Figura 9 – Fatores Motivadores da Governança de TI**



Para o gerenciamento das TIC foram desenvolvidos modelos de Governança de Tecnologia da Informação e Comunicações tendo em vista os benefícios, oportunidades e riscos desta área. A alta gerência da organização pública deve estar informada no que diz respeito às melhores práticas de Governança de TI para conseguir o máximo de aproveitamento dos investimentos realizados em TIC garantir a sua segurança. Não se deseja gastar mais que o necessário nesse processo e por isso a forma como a TI é governada é essencial para não prejudicar a estrutura e funcionamento dos órgãos do governo, valendo-se de que a segurança cibernética seja a causa de grande parte dos riscos das organizações.

O retorno dos investimentos realizados em TI é verificado por meio de medições, avaliações e monitoramento, a fim de garantir que a estratégia de Governança de TI esteja de acordo com o foco da organização ou se haja a necessidades de modificações ou de novos investimentos. Essa ligação entre TI e organização dá ensejo a resultados importantes para aplicações específicas e necessárias como é o caso da segurança cibernética na Administração Pública Federal.

Referindo-se às decisões, responsabilidades e ações relativas à TI, de um modo geral, no âmbito da organização, a Governança de TI deve dar suporte para prescrever a administração objetiva. Dentre tantas decisões, está presente a

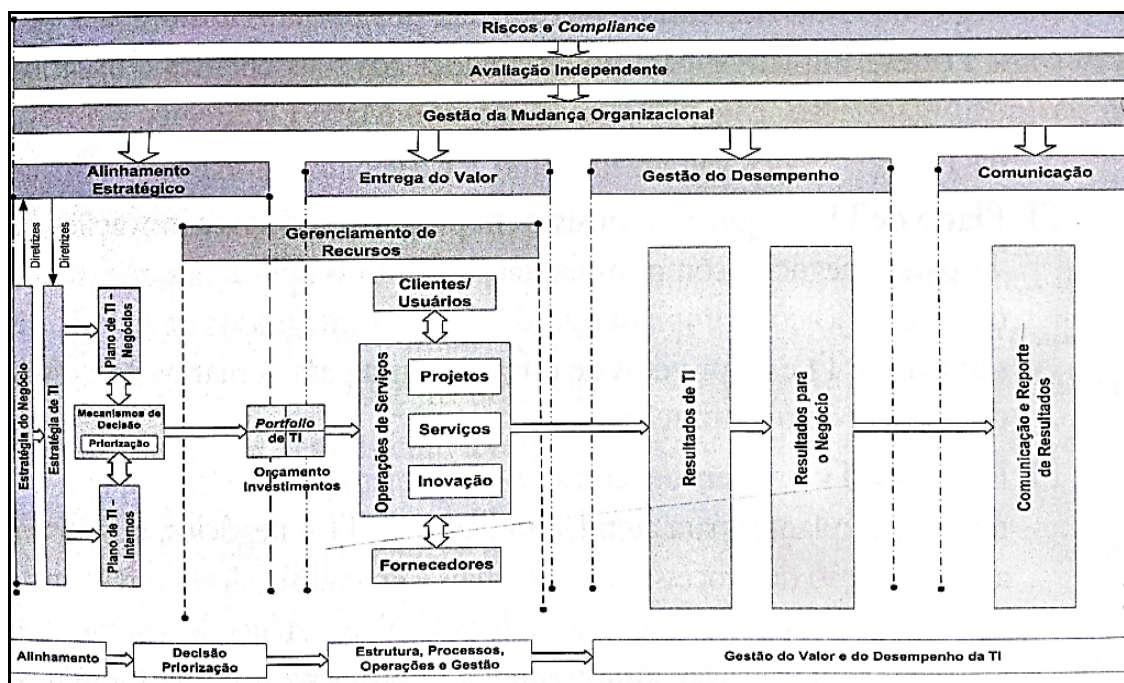


segurança da informação, a qual pode estar embasada em um modelo associado à própria segurança.

A segurança da informação e as necessidades da organização referente a ela são relacionadas pela prática, cada vez mais adotada internacionalmente, chamada de Governança da Segurança da Informação. Seu objetivo é que os sistemas de informações atendam aos critérios de integridade, disponibilidade, confidencialidade e autenticidade. As áreas gerenciais e operacionais de segurança da informação atuam de maneira mais eficiente nesse sentido com o uso de modelos de Governança de TI mais adequados às reais necessidades das organizações.

Um modelo genérico pode e deve ser adaptado para a organização onde será implantado e desenvolvido segundo as suas prioridades, necessidades e disponibilidades (FERNANDES et al., 2012). No entanto, para que tudo ocorra, são necessárias amplas negociações na alta administração e capacitação dos gerentes de cada área, os quais carecerão de habilidades para que os desafios sejam superados.

Figura 10 – Visão geral do modelo de Governança de TI.



Fonte: (FERNANDES, et al. p. 41).

### 2.4.1. Modelo COBIT

O COBIT (*Control Objectives for Information and Related Technology*) foi produzido inicialmente em 1994 pela ISACF e desde então vem sofrendo atualizações à medida em que surgem padrões internacionais técnicos, profissionais, regulatórios e específicos para processos de TI aptos a serem adicionados (FERNANDES et al., 2012). A última atualização ocorreu em 2007, quando foi realizado um refinamento dos objetivos de controle dos processos de verificação e divulgação dos resultados, passando a vigorar a versão 4.1.

Ele é utilizado pela área de TI como um guia de boas práticas, concordante com os melhores padrões, por meio de modelos de domínios e processos, mais concentrados nos controles do que na execução, a fim de dar suporte para as organizações colocarem em funcionamento uma governança efetiva de sua TI. Muitos o consideram como base da Governança tecnológica; ele atua como um padrão e oferece qualidade, níveis de maturidade, segurança da informação, tudo isso com a formalização de métodos para área de TI das organizações (BERNARD e MOREIRA, 2005).

De acordo com IT Governance Institute (2007, p. 11), a missão do COBIT é:

Pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado dia-a-dia por gerentes de negócios, profissionais de TI e profissionais de avaliação.

Todos os componentes são inter-relacionados para alcançar o principal objetivo de sua aplicação, que é a entrega de produtos e serviços de TI a partir das necessidades, relacionando requisitos de governança e de negócios. Nesse sentido, os executivos devem pôr em prática essa metodologia, que abrange os processos mais comuns relativos às funções da TI e são compreensíveis em todos os níveis, tornando, assim, os objetivos da alta administração conectados aos trabalhos realizados operacionalmente.

As áreas de foco na governança de TI (figura 11) que o COBIT sustenta descrevem os cinco tópicos que devem ser alvos de atenção por parte dos executivos das organizações.

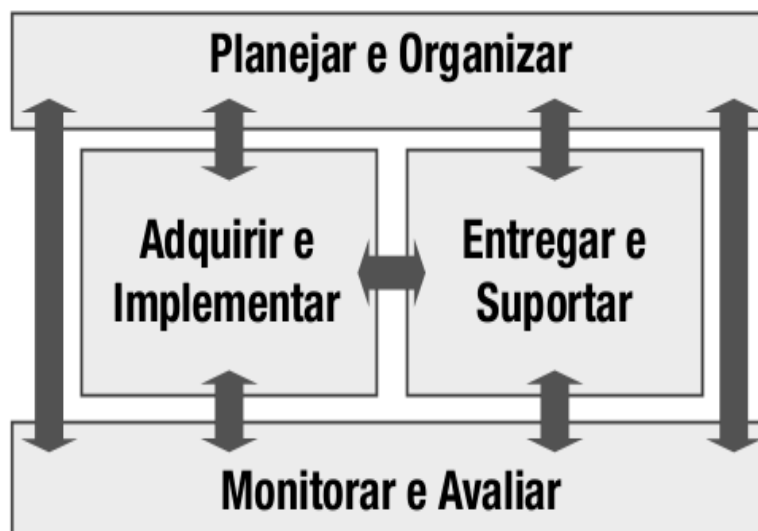
Figura 11 - Áreas-Foco da Governança de TI, na visão do COBIT.



Fonte: (ITGI, 2007).

O COBIT é um modelo de gestão orientado a processos. Está constituído por quatro domínios por onde estão distribuídos os seus trinta e quatro processos de TI. Cada domínio é associado a amostras do que existe em uma organização de TI modelo e, desta forma, permitem gerenciar as informações com recursos de TI para que os executivos tenham objetivos e controles que o ajudem a definir a meta de configuração de políticas, planos e procedimentos, bem como a estrutura organizacional (ITGI, 2007).

Figura 12 - Domínios inter-relacionados do COBIT.



Fonte: (ITGI, 2007).

De acordo com Fernandes e Abreu (2012), os quatro domínios do COBIT são descritos como:

**Planejamento e Organização (PO)** – possui 10 processos com objetivos estratégicos e táticos, e identifica as melhores formas com que a TI pode contribuir para atender aos objetivos de negócio, envolvendo planejamento, comunicação e gerenciamento em diversas perspectivas.

**Aquisição e Implementação (AI)** – possui 7 processos que cobrem identificação, desenvolvimento e/ou aquisição de soluções de TI para executar a estratégia diretiva do Plano Diretor de Informática (PDI), bem como sua implementação e integração junto aos processos de negócio. Mudanças e manutenções em sistemas existentes também estão cobertas por este domínio, para garantir a continuidade dos respectivos ciclos de vida.

**Entrega e Suporte (DS)** – possui 13 processos para entrega e atendimento dos serviços requeridos, incluindo gerenciamento de segurança e continuidade, suporte aos serviços para os usuários, gestão dos dados e da manutenção da infraestrutura operacional.

**Monitoração e Avaliação (ME)** – possui 4 processos que visam a assegurar a qualidade dos processos de TI, assim como a governança e validação da eficiência

dos processos de auditoria, por meio de mecanismos regulares de acompanhamento, monitoração de controles internos e de avaliações internas e externas.

Para decisões sobre valor, riscos e controles, as organizações fazem uso de ferramentas de gerenciamento como, painel de controle, “scorecards” e “benchmarking” para encontrar as respostas de que precisam. Os produtos COBIT estão organizados em três níveis que dão suporte a: Executivos e Alta Direção; Gerentes de TI e de Negócios; Profissionais de avaliação, controles e segurança.

O COBIT trata a questão níveis de maturidade, semelhante ao modelo CMM (Capability Maturity Model for Software), que permite com que a organização visualize sua situação atual para um monitoramento mais sistemático e identifique a profundidade mais adequada para aplicar mecanismos de controle e desempenho.

Modelos de Maturidade (FERNANDES et al., 2012):

**Tabela 2- Modelos de maturidade.**

<b>Nível de Maturidade</b>	<b>Estágio do Processo</b>
<b>0 – Inexistente</b>	Processos de Gestão não aplicados.
<b>1 – Inicial</b>	Processos são desorganizados e não planejados.
<b>2 – Repetitivo</b>	Processos regulares e dependentes dos conhecimentos dos funcionários.
<b>3 – Definido</b>	Processos são padronizados, documentados e documentados na organização.
<b>4 – Gerenciado e Mensurável</b>	Processos são monitorados e medidos quanto à conformidade com os procedimentos, e ações são tomadas quando os resultados não são efetivos.
<b>5 – Otimizado</b>	Processos são melhorados continuamente com uso de automação e são seguidas as melhores práticas do mercado.

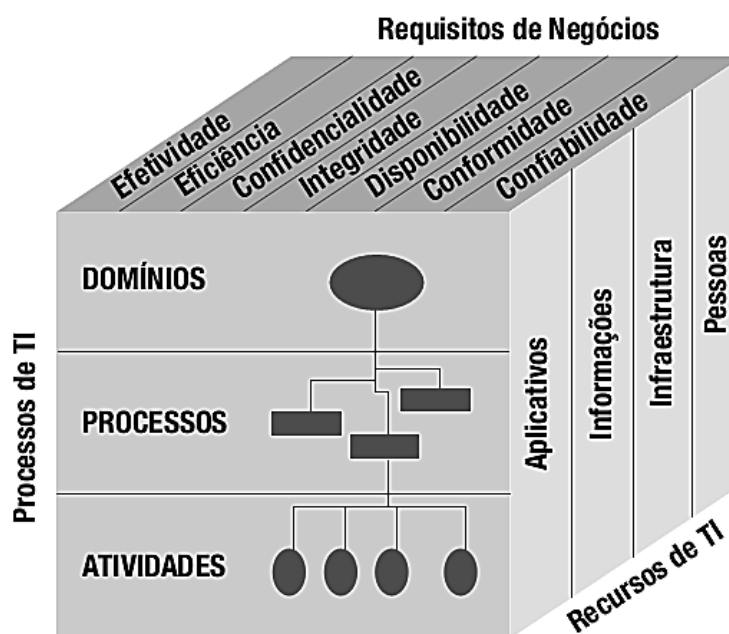
O resultado do uso desse modelo de maturidade proporciona a alta gerência condições (FERNANDES; ABREU, 2008) de:

- mapear a situação atual da organização;
- comparar a situação das melhores organizações no segmento (*benchmarking*);

- comparar padrões internacionais;
- estabelecer e monitorar passo a passo as melhorias dos processos rumo à estratégia da organização.

Uma visão integrada do COBIT é representada na figura abaixo (ITGI, 2007) na qual se visualiza o seu princípio básico de funcionamento na forma em que os **recursos** são gerenciados por **processos** para atingir **metas**, as quais estão relacionadas intimamente aos **requisitos de negócio**.

Figura 13 - Cubo COBIT.



Fonte: (ITGI, 2007).

No que se refere à Governança de Segurança da Informação, o COBIT fornece normas que garantem que todos os elementos de segurança integrem a estratégia de segurança da informação na organização.

Pelos motivos apresentados, o COBIT é um modelo reconhecido e bastante empregado mundialmente por gerentes de informática e auditores de TI.

## 2.4.2. Modelo ITIL

Um esforço para disciplinar e permitir a comparação entre as propostas dos diversos proponentes prestadores de serviços de TI para o governo britânico, a ITIL

(*Information Technology Infrastructure Library*) foi formada pela CCTA (*Central Communications and Telecom Agency*), que atualmente é a OGC (*Office of Government Commerce*). Em pouco tempo, devido a sua disponibilidade gratuita, foi amplamente adotada pelas organizações da Europa e América do Norte; atualmente, é considerada um padrão no segmento de TI (MAGALHAES; PINHEIRO, 2007).

A ITIL se encontra na versão três (V3), lançada em maio de 2007, cuja organização dos processos de gerenciamento de serviços foi modificada para estrutura de ciclo de vida de serviço, o que representa uma evolução em relação à versão anterior (FERNANDES et al., 2012).

Serviço de TI, para a ITIL, representa um ou mais sistemas de TI que habilitam um processo de negócio. O serviço de TI é gerenciado com a integração dos elementos deste sistema, com objetivo na sua entrega e suporte, mantendo o foco nas necessidades dos clientes e de acordo com a estratégia da organização.

Os processos para suporte e entrega dos serviços de TI apresentados pelo ITIL podem ser classificados de acordo com a Figura 14 (MAGALHÃES et al., 2007).

**Figura 14 - Posicionamento processos da ITIL.**



**Fonte: (MAGALHÃES et al., 2007, p. 66).**

As melhores práticas de Gerenciamento de Serviços de TI formam o modelo ITIL o qual propõe uma metodologia centrada nesses processos e nas suas relações de dependência, em um ambiente de qualidade. Tem o propósito de realizar a

melhoria contínua do gerenciamento da área de TI como negócio da organização, na qual se inclui pessoas, processos e tecnologia. É considerado o caminho mais promissor para aumentar o desempenho no gerenciamento dos serviços de TI e dessa forma manter em sintonia a área de TI com as áreas de negócio e estratégicas da organização (MAGALHAES; PINHEIRO, 2007).

Com base em um estudo realizado pelo Gartner Group, Inc. foram definidos os níveis de maturidades relacionados aos processos dos negócios em que se descreve:

**Tabela 3 – Níveis de Maturidade PCN**

NÍVEIS	DESCRIÇÃO
<b>0 – Não existe</b>	<ul style="list-style-type: none"> <li>• Pouca ou nenhuma documentação;</li> <li>• Inexistência de abordagem ou comprometimento corporativo;</li> <li>• A necessidade é vista como um problema da área de TI.</li> </ul>
<b>1 – Inicial</b>	<ul style="list-style-type: none"> <li>• Poucos executivos reconhecem que o PCN é um problema a ser estudado;</li> <li>• Inexistência de abordagem estruturada;</li> <li>• Diferentes grupos utilizam diferentes abordagens, sem usar nenhuma metodologia;</li> <li>• Existência de investimento, porém sem relatórios ou controles.</li> </ul>
<b>2 – Repetitivo</b>	<ul style="list-style-type: none"> <li>• Existe um reconhecimento dos executivos da necessidade do PCN;</li> <li>• Existem regras formais para o PCN, porém sem métricas;</li> <li>• Sistemática para desenvolvimento e manutenção de PCNs;</li> <li>• O PCN é encarado como um projeto, e não como um processo;</li> <li>• Foco é desastre em TI.</li> </ul>
<b>3 – Definido</b>	<ul style="list-style-type: none"> <li>• Processos e procedimentos estão padronizados e documentados, porém sem controle se, de fato serão cumpridos;</li> <li>• Estrutura formal de PCN – responsáveis;</li> <li>• Execução regular de testes e exercícios;</li> </ul>



NÍVEIS	DESCRIÇÃO
	<ul style="list-style-type: none"> <li>• Foco é TI e funções críticas do negócio;</li> <li>• Existência de orçamento para PCN.</li> </ul>
<b>4 - Gerenciado</b>	<ul style="list-style-type: none"> <li>• PCN é previsto como parte do gerenciamento de riscos;</li> <li>• Execução de Controles;</li> <li>• PCN visto como processo, e não como projeto;</li> <li>• Processos são revisados periodicamente para melhorias, melhores práticas.</li> </ul>
<b>5 – Otimizado</b>	<ul style="list-style-type: none"> <li>• PCN discutido nos altos níveis da organização;</li> <li>• Gerenciamento de risco faz parte da cultura da organização;</li> <li>• PCN focado nos processos de negócio e na cadeia de suprimentos;</li> <li>• PCN incluído no início dos projetos de TI;</li> <li>• Exercício e testes regulares dos procedimentos do PCN são executados corporativamente.</li> </ul>

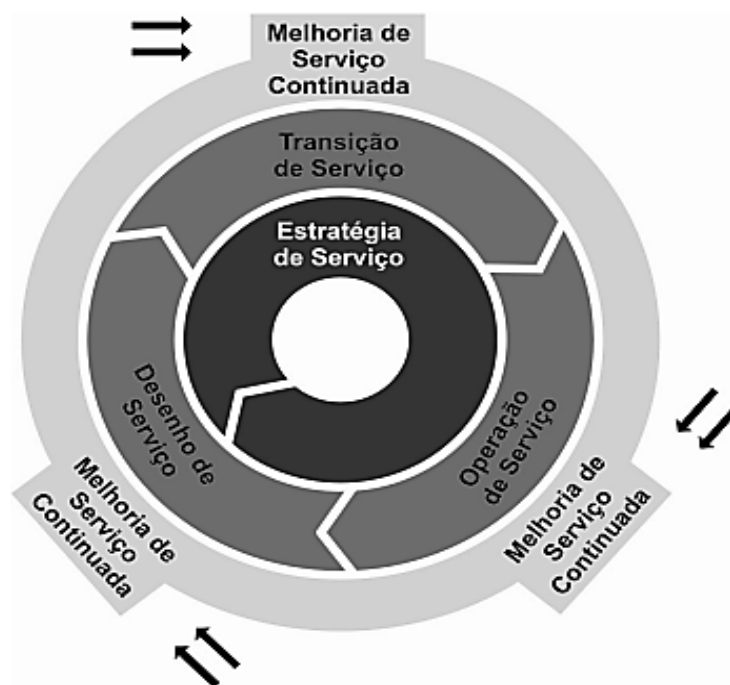
O dimensionamento do trabalho relacionado ao Gerenciamento de continuidade dos serviços de TI é identificado nos níveis de maturidade.

Operação e gestão da infraestrutura de TIC é o escopo de atuação do modelo ITIL no qual demonstra as melhores práticas sobre os processos que podem ser utilizados como base para definir os processos a serem colocados em funcionamento pela organização como melhor convier. Por meio dos processos padronizados de gerenciamento de serviços se adquire uma correta adequação entre os níveis de serviços oferecidos pela área de TI e o quanto se paga por ela. É possível diminuir os custos e ainda aumentar a qualidade oferecida aos usuários.

Em uma visão estruturada do modelo ITIL, ele pode ser dividido em dois componentes (

Figura 15) o Núcleo do ITIL, que contém a publicação das orientações quanto a melhores práticas, e a orientação complementar, que é um conjunto de publicações complementares para utilização das práticas do núcleo em setores empresariais diversos. As cinco publicações do Núcleo da ITIL se relacionam com uma fase do ciclo de vida do serviço (Tabela 4), e em cada um há orientações para tratamento integrado de gerenciamento de serviços (FERNANDES; ABREU, 2008).

Figura 15 – O Núcleo da ITIL.



Fonte: (FERNANDES et al., 2012, p. 258).

Tabela 4 - Publicações, processos e Orientações da ITIL.

Publicações	Processos	Orientações
<b>Estratégia de Serviço</b>	<ul style="list-style-type: none"> <li>Gerenciamento Financeiro de TI;</li> <li>Gerenciamento do Portfólio de Serviços;</li> <li>Gerenciamento da Demanda.</li> </ul>	Sobre políticas e processos de gerenciamento de serviço ao longo do ciclo de vida de serviço.
<b>Desenho de Serviço</b>	<ul style="list-style-type: none"> <li>Gerenciamento do Catálogo de Serviços;</li> <li>Gerenciamento do Nível de Serviço;</li> <li>Gerenciamento da Capacidade;</li> <li>Gerenciamento da disponibilidade;</li> <li>Gerenciamento da Continuidade de Serviço;</li> <li>Gerenciamento de Segurança da Informação;</li> <li>Gerenciamento de Fornecedor.</li> </ul>	Para desenho e desenvolvimento dos serviços e dos processos de gerenciamento dos serviços, detalhando gerenciamento do catálogo de serviços, nível do serviço, capacidade, disponibilidade, continuidade e <u>segurança da informação</u> e dos fornecedores, além de mudanças e de melhorias necessárias.
<b>Transição de Serviço</b>	<ul style="list-style-type: none"> <li>Gerenciamento de Mudança;</li> <li>Gerenciamento de Configu-</li> </ul>	Sobre efetivação da transição de serviços novos e modifi-

<b>Publicações</b>	<b>Processos</b>	<b>Orientações</b>
	ração e de Ativo de Serviço; <ul style="list-style-type: none"> <li>• Gerenciamento da Liberação e Implantação;</li> <li>• Validação e Teste de Serviço;</li> <li>• Avaliação;</li> <li>• Gerenciamento do Conhecimento;</li> </ul>	cados.
<b>Operação de Serviço</b>	<ul style="list-style-type: none"> <li>• Gerenciamento de Evento;</li> <li>• Gerenciamento de Incidente;</li> <li>• Gerenciamento de Requisição;</li> <li>• Gerenciamento de Problema;</li> <li>• Gerenciamento de Acesso.</li> </ul>	Sobre garantir a entrega e suporte a serviços de forma eficiente e eficaz.
<b>Melhoria de Serviço Continuada</b>	<ul style="list-style-type: none"> <li>• Relatório de Serviço;</li> <li>• Medição de Serviço.</li> </ul>	Sobre melhorias na qualidade dos serviços, nas metas, na continuidade etc, baseado na ISO 20000.

Este modelo de gerenciamento pode ser aplicado a uma organização da APF, já que, uma vez estabelecido o plano de ação, ao longo de sua execução, os processos de TI são controlados por meio de mecanismos adequados que visem a seu desenvolvimento e maturidade.

### **2.4.3. Modelos ABNT NBR ISO/IEC 17799:2005**

Os avanços tecnológicos sendo aplicados cada vez mais na automação de compartilhamento de informações despertaram o interesse das organizações pela formação de uma norma de acordo com as características de aplicação na gestão de segurança da informação com fins de estabelecer um modelo comum (SÊMOLA, 2003).

Para atender a esse interesse de empresas, governos e instituições, a norma BS 7799 foi criada pelo *British Standards Institute* (BSI) em 1989, tendo dois objetivos principais: prestar auxílio a fornecedores de produtos de segurança de TI a partir de critérios de avaliação e programa de certificação, e auxiliar usuários de TI por meio do uso de um Código de Prática do Usuário. Seu aperfeiçoamento deu origem ao Código de Prática para Gestão da Segurança da Informação, BS 7799-1:1995 parte1 (FERNANDES et al., 2012).

Posteriormente, a fim de permitir a certificação de um sistema gerencial de

segurança da informação, pois a parte 1 da BS 7799 era somente um código de prática, foi lançada em 2002 a parte 2 da BS 7799 (BS 7799-2:2002).

Tais normas tiveram uma substituição elaborada pela Comissão de Estudo de Segurança Física em Instalações de Informática, no Comitê Brasileiro de Computadores e Processamento de Dados, e lançada em outubro de 2005 (ABNT, 2005). Foi implantado um novo esquema de numeração da norma, sendo transformadas a BS 7799-1 e BS 7799-2 respectivamente em ISO/IEC 27002 e ISO/IEC 27001, mantendo a equivalência do conteúdo (ABNT, 2005).

Segundo Fernandes e Abreu (2012, p. 412), são os objetivos dos modelos ISO/IEC 27001 e 27002:

A ISO/IEC 27001 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 à avaliação da conformidade por partes interessadas internas e externas.

A ISO/IEC 27002 estabelece diretrizes e princípios gerais para iniciar, manter e melhorar a gestão da segurança da informação em uma organização, fornecendo direcionamento sobre as metas geralmente aceitas para a gestão da segurança da informação. A implantação dos objetivos de controle e dos controles associados da norma tem como finalidade atender aos requisitos identificados por meio da análise/avaliação de riscos. Outro objetivo da norma é servir como um guia prático para desenvolver os procedimentos de segurança da informação e práticas eficientes de gestão da segurança para informação, além de ajudar a criar confiança nas atividades interorganizacionais.

Esses objetivos da norma ajudam a analisar a Governança da Segurança da Informação nos órgãos da APF, pois nos oferece o enfoque necessário para identificar os processos adotados pelo governo federal.

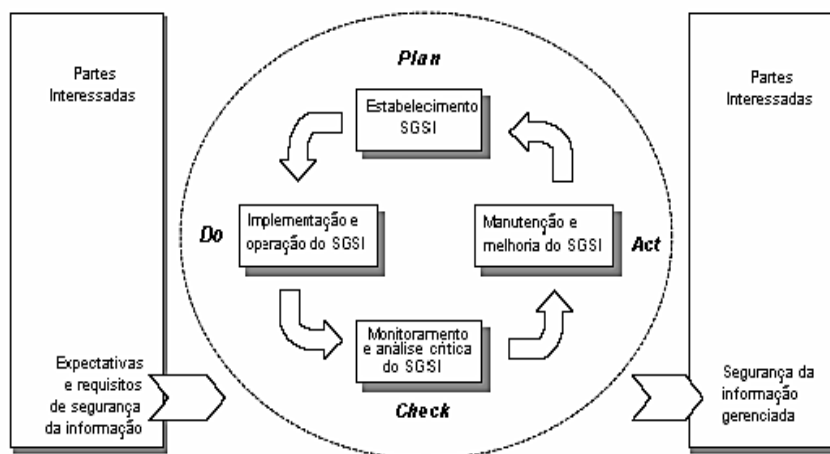
A norma **ISO/IEC 27001**, em sua abordagem de processo para gestão da segurança da informação, estimula que os usuários destaquem a importância de:

- entender os requisitos de segurança da informação de uma organização e a necessidade de estabelecer uma política e objetivos para a segurança de informação;
- implementar e operar controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;
- monitorar e analisar criticamente o desempenho e eficácia do Sistema de Gestão de Segurança da Informação - SGSI; e

- promover a melhoria contínua baseada em medições objetivas.

Ela adota o modelo conhecido como ciclo PDCA (*Plan-Do-Check-Act*) que é aplicado para estruturar todos os processos do SGSI. A Figura 16 ilustra como um SGSI considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a esses requisitos e expectativas.

**Figura 16 - Modelo PDCA aplicado ao SGSI.**



Fonte: (ABNT, 2006)

A norma está estruturada em cinco seções sob o ponto de vista operacional (FERNANDES, et al., 2012):

- o sistema de gestão de segurança da informação, dentro dos critérios do PDCA do SGSI e dos requisitos de documentação;
- a responsabilidade da administração;
- auditorias internas do SGSI;
- a melhoria do SGSI.

A norma **ISO/IEC 27002** está estruturada em 11 seções, reunidas em 39 categorias principais de segurança e uma seção introdutória tratando sobre análise e tratamento de riscos. As categorias se desdobram em um total de 132 controles (ABNT, 2007). A descrição de cada controle está acompanhada de sua definição, das diretrizes para implementação e, quando possível, de informações adicionais,

por exemplo, as considerações legais e as referências normativas.

As seções colocadas são as seguintes:

- política de Segurança da Informação;
- organizando a Segurança da Informação;
- gestão de Ativos;
- segurança de Recursos Humanos;
- segurança Física e do Ambiente;
- gestão de Operações e Comunicações;
- controle de Acesso;
- aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- gestão de Incidentes de Segurança da Informação;
- gestão de Continuidade do Negócio;
- conformidade.

Aderir a essas normas como modelos para segurança da informação demonstra um comprometimento dos órgãos com a proteção, confidencialidade, integridade e disponibilidade das informações. Seus controles podem ser inseridos em implantação e administração de sistemas de redes, guias para implantação de políticas de segurança, planos de continuidade do negócio e aderência às legislações.

#### **2.4.4. Modelo PMBOK**

O PMBOK (*Project Management Body of Knowledge*) é um notável Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos elaborado por diversos profissionais pertencentes ao PMI (*Project Management Institute*), organização não governamental referência mundial na gestão de projetos. Ele é utilizado como um documento formal para descrição de normas, métodos, processos e práticas. A área de TIC é caracterizada por constantes evoluções por isso o documento passa por revisões nas quais recomendações de valor são adequadas e incorporadas a cada versão. Atualmente encontra-se na versão número quatro, cujo lançamento ocorreu no ano de 2008.

O objetivo do PMBOK é identificar os relevantes conhecimentos de um total

existente sobre gerenciamento de projetos que sejam amplamente reconhecidos, ou seja, aplicáveis a grande maioria dos projetos. Ele fornece um aspecto geral das habilidades, ferramentas e técnicas relativas à profissão de Gerente de Projetos que são fatores críticos ao sucesso (PMI, 2008).

O PMBOK (2008) descreve os conceitos basilares para o gerenciamento de projetos, são eles:

#### Projeto:

Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. A sua natureza temporária indica um início e um término definidos. O término é alcançado quando os objetivos tiverem sido atingidos ou quando se concluir que esses objetivos não serão ou não poderão ser atingidos e o projeto for encerrado, ou quando o mesmo não for mais necessário. [...].

#### Gerenciamento de projetos:

O gerenciamento de projetos é a aplicação de conhecimento, habilidades, ferramentas e técnicas às atividades do projeto a fim de atender aos seus requisitos. [...].

#### Escritório de projetos

Um escritório de projetos (Project Management Office, PMO) é um corpo ou entidade organizacional à qual são atribuídas várias responsabilidades relacionadas ao gerenciamento centralizado e coordenado dos projetos sob seu domínio. As responsabilidades do PMO podem variar desde fornecer funções de suporte ao gerenciamento de projetos até ser responsável pelo gerenciamento direto de um projeto.

#### Gerente de projetos:

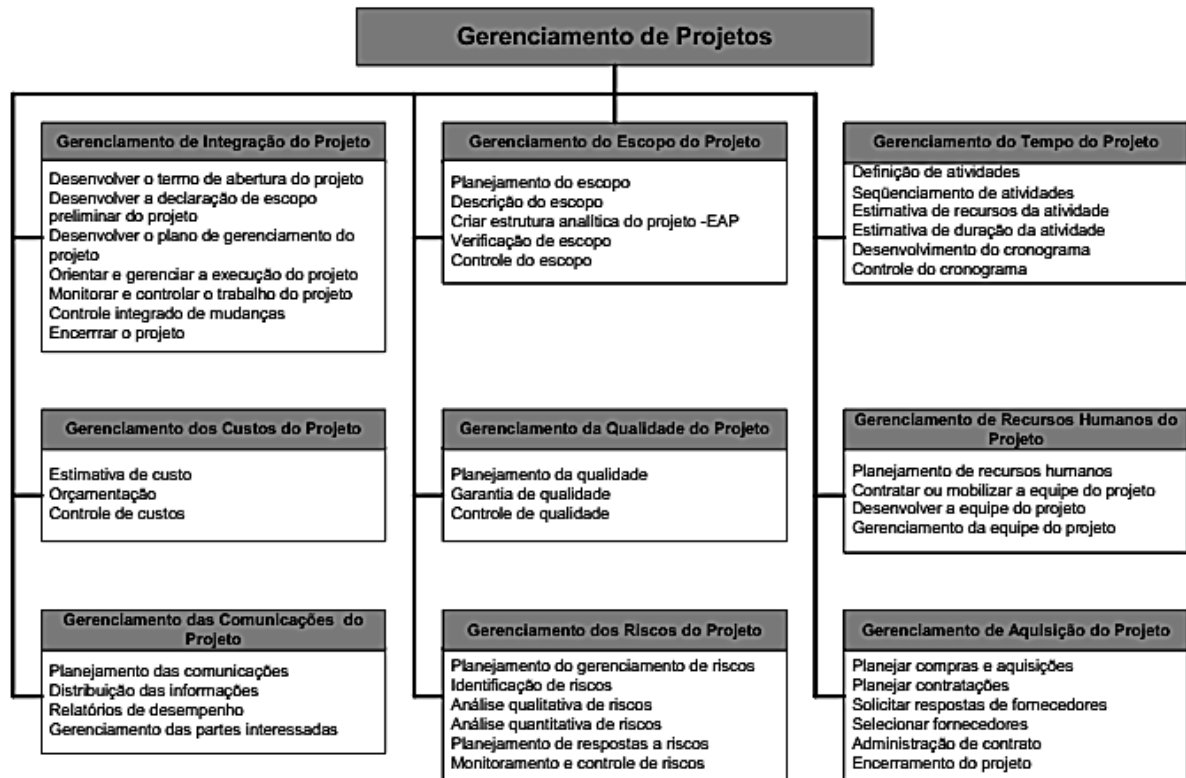
O gerente de projetos é uma pessoa designada pela organização executora para atingir os objetivos do projeto. O papel do gerente de projetos é diferente de um gerente funcional ou gerente de operações. [...].

O modelo PMBOK está estruturado em 9 áreas do conhecimento em gerenciamento de projetos (



Figura 17) contendo as atividades com o conteúdo correlato.

Figura 17 - Áreas do conhecimento do PMBOK.



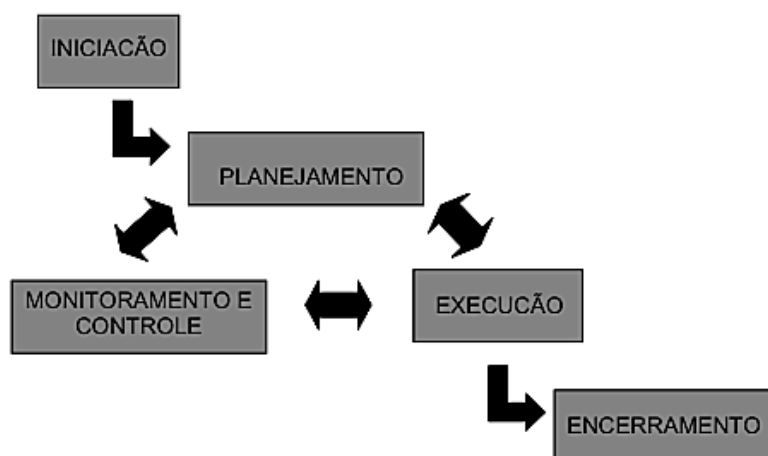
Fonte: (PMI, 2008).

Essas áreas do conhecimento agrupam os processos em fases que se relacionam conforme o ciclo de vida do projeto (

Figura 18):

- Iniciação - define e autoriza o projeto ou uma fase do projeto.
- Planejamento – define e refina os objetivos, e planeja ações necessárias para alcançar objetivos e escopo para os quais o projeto foi idealizado;
- Execução – integra pessoas e outros recursos para realizar o plano de gerenciamento do projeto;
- Monitoramento e Controle – mede e monitora regularmente o progresso para identificar variações em relação ao plano de gerenciamento do projeto, visando à tomada de ações corretivas;
- Encerramento – formaliza a aceitação do produto, serviço ou resultado e conduz o projeto ou uma fase do projeto a um final ordenado.

**Figura 18 - Relação entre os grupos de processos.**



Visto como disciplina da Governança de TI, os conhecimentos de gerenciamento de projetos apresentados pelo guia PMBOK, são bastante úteis para projetos de TI da APF na implantação de um modelo de Gestão de Segurança da Informação. Eles dispõem de providências a respeito do gerenciamento de implementação de novos elementos ou modificações no contexto da segurança cibernética.

### **3. GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS DA APF**

Todos desejam que os nossos dados e os de segurança nacional do governo estejam bem protegidos. Em contrapartida, são muitos os casos de falhas recentes ocorridas na segurança em órgãos públicos no Brasil e no exterior que nos deixam alarmados. Alguns desses fatos são estudados ao final deste documento.

É importante salientar que o país não está alheio a tais fatos; está buscando coordenar as atividades de segurança de infraestruturas críticas da informação dentro da realidade atual. Assim, para agir em prol da segurança da informação e comunicações, visando a garantir a disponibilidade, integridade, confidencialidade e autenticidade no campo de ação da Administração Pública Federal, direta e indireta; vêm sendo realizados estudos técnicos especializados e criados grupos de trabalho, incluindo diversas publicações, para melhor garantir a Segurança Nacional (DSIC,

2010).

Muitas dessas publicações geradas, às quais se permitiram o acesso, foram utilizadas como base para construção desta parte do trabalho que apresenta como os dados sensíveis são gerenciados pelo governo brasileiro, visando a garantir a continuidade da prestação de serviços, mesmo em situação de crise.

### **3.1. Administração Pública Federal**

Alexandrino e Paulo (2011) citam a administração pública em sentido amplo e sentido estrito. No sentido amplo, a administração pública inclui os órgãos do governo que exercem função política, e também os órgãos e pessoas jurídicas que exercem função meramente administrativa. No sentido estrito, só inclui os órgãos e pessoas jurídicas que exercem função meramente administrativa, de execução dos programas de governo. O governo representa o conjunto de órgãos constitucionais responsáveis pela função política do Estado. Relaciona-se com função política de comando, de coordenação, de direção e de fixação de planos e diretrizes de atuação do Estado.

O conceito de governo difere do conceito de administração pública no sentido estrito, sendo este o mais aplicável a este trabalho em virtude de tratarmos de ações cibernéticas que atentam contra a infraestrutura dos órgãos que executam atividades do Governo Federal.

O governo exerce a direção suprema do Estado, determinando como serão realizados os objetivos e as diretrizes dos planos governamentais para soberania da nação, por intermédio dos órgãos públicos criados e regulados de acordo com a Constituição Federal (ALEXANDRINO, et al., 2011).

O sistema atual de governo, o presidencialista, confere a divisão dos poderes para o Executivo, Legislativo e Judiciário, de modo que sejam independentes e harmônicos entre si. O presidente da República, como chefe do Poder Executivo Federal, exerce a direção maior da Administração Pública Federal, sendo-lhe atribuído a sua organização e estruturação conforme previsto na Constituição Federal (ALEXANDRINO, et al., 2011).

O artigo 4º do Decreto-Lei 200 (1967, apud Alexandrino & Paulo, 2011, p.28) mostra a organização da Administração Pública Federal tal qual se conhece,

conforme disposto abaixo:

Art. 4º A Administração Federal compreende:

I - A Administração Direta, que se constitui dos serviços integrados na estrutura administrativa da Presidência da República e dos Ministérios.

II - A Administração Indireta, que compreende as seguintes categorias de entidades, dotadas de personalidade jurídica própria:

- a) Autarquias;
- b) Empresas Públicas;
- c) Sociedades de Economia Mista.
- d) Fundações públicas.

Parágrafo único. As entidades compreendidas na Administração Indireta vinculam-se ao Ministério em cuja área de competência estiver enquadrada sua principal atividade.

O Decreto-Lei 200 (1967) rege ainda os princípios fundamentais do planejamento, da coordenação, da descentralização e da delegação de competências entre eles, conforme o disposto em seu artigo 30:

Art. 30. Serão organizadas sob a forma de sistema as atividades de pessoal, orçamento, estatística, administração financeira, contabilidade e auditoria, e serviços gerais, além de outras atividades auxiliares comuns a todos os órgãos da Administração que, a critério do Poder Executivo, necessitem de coordenação central.

À medida que os processos administrativos da administração pública foram se tornando ao longo do tempo mais dependentes da tecnologia de informática esta se inseriu como sistema imprescindível para o governo. Um exemplo é o Serviço Federal de Processamento de Dados – SERPRO, cuja missão é modernizar e dar agilidade a setores estratégicos da Administração Pública; ele é considerado uma das maiores organizações públicas de TI no mundo (SERPRO, 2012).

A administração pública é composta por (DSIC, 2010):

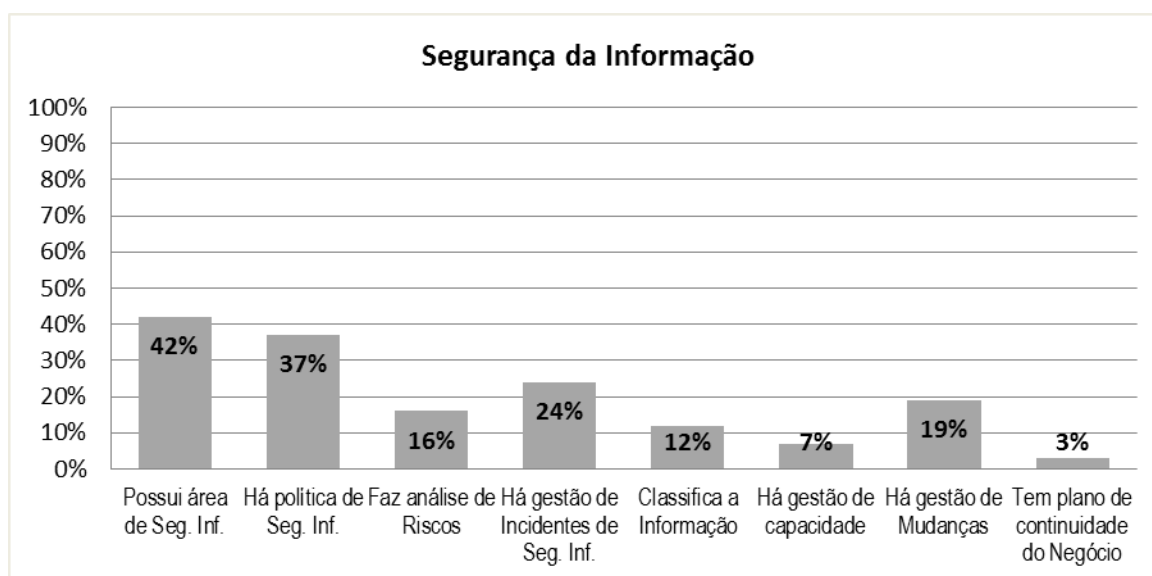
- 39 Ministérios (incluindo secretarias e órgãos com status de ministério);
- Aproximadamente 6.000 entidades governamentais;
- Aproximadamente 950.000 servidores federais;
- Aproximadamente 320 grandes redes do governo federal;
- Aproximadamente 12.000 sites “.gov.br”.

A complexidade dos sistemas informatizados em sua aplicação na administração pública traz consigo os problemas de segurança a qual passa a ser matéria legislativa. Foram abordados pela primeira vez no Decreto nº 3.505 (2000), que institui a política de segurança da informação nos órgãos e entidades da APF.

Legislações e órgãos relacionados com a segurança das informações e comunicações na APF são tratados em tópicos específicos. Porém, cabe citar aqui, que mesmo com todas essas medidas criadas até hoje, um levantamento acerca da governança de TI realizado pelo Tribunal de Contas da União – TCU, em 2010 (BRASIL, 2010), com 315 órgãos/entidades das administrações direta e indireta apontou vulnerabilidades das redes do governo. Nele é mapeado o estado da Governança de TI de acordo com os aspectos de planejamento estratégico, desenvolvimento de software, gestão de níveis de serviço, processo de contratação e gestão de TI, processo orçamentário e auditoria de TI.

A Figura 19 apresenta os dados relacionados à prática de segurança da informação e comunicações na APF (BRASIL, 2010).

**Figura 19 - Indicadores de Segurança da Informação na APF.**



**Fonte: (BRASIL,2010)**

Em 2011, o Orçamento da União para os gastos com recursos de TI foram de R\$ 18 bilhões (PACHECO, 2011). Espera-se que esse valor seja aplicado de modo eficiente; porém, no mesmo relatório, um fator chama a atenção: o fato de que em 51% das unidades a alta administração não se responsabiliza pelas políticas de TI, restringindo a responsabilidade apenas aos profissionais da área (BRASIL, 2010). Esse fato representa um equívoco na estrutura da governança de TI, uma vez que os representantes máximos das instituições públicas devem ter responsabilidade da

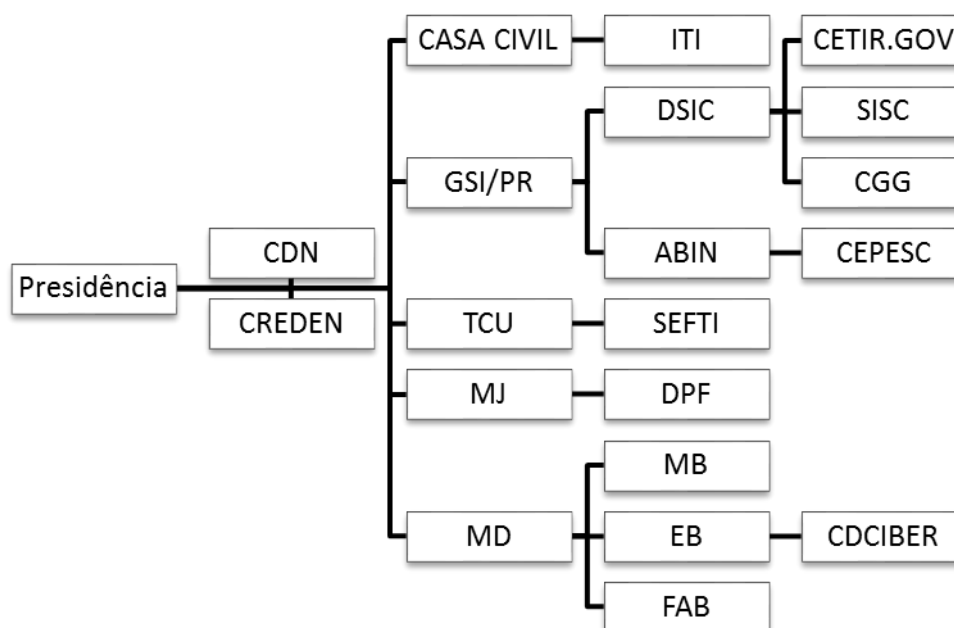
gestão de TI para tornar os sistemas das esferas federais menos vulneráveis.

No relatório do levantamento, o próprio ministro-relator Aroldo Cedraz faz a seguinte afirmação: “Os dados coletados não deixam margem à dúvida de que a situação da governança de TI na Administração Pública Federal ainda se encontra em estado precário” (BRASIL, 2010, p. 40).

### 3.2. Órgãos estratégicos para Segurança e Defesa Cibernética

É importante salientar que todos os órgãos e funcionários da APF têm relação com a segurança cibernética, porém aqui são apontados aqueles que estão envolvidos ativamente na estratégia de defesa cibernética adotada para o país, relacionando suas atribuições/funções com suas principais ações no campo deste estudo.

Figura 20 - Hierarquia dos principais órgãos da APF na segurança e defesa cibernética.



Os assuntos relacionados à segurança da informação e comunicações, segurança cibernética e segurança das infraestruturas críticas no âmbito nacional estão sob o domínio do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN).

O CDN é um órgão de consulta da Presidência para assuntos relacionados



com a soberania nacional e defesa do Estado democrático e desta forma atua em decisões estratégicas também em questões cibernéticas.

Já o CREDEN é um órgão de assessoramento da Presidência para assuntos pertinentes às relações exteriores e à defesa nacional. Em suas atribuições estão incluídas a segurança das informações e comunicações bem como a segurança cibernética no que tange a diretrizes estratégicas.

Ambos utilizam como Secretaria-Executiva o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Em uma reunião do CREDEN, foi decidida a criação do Comitê Gestor da Informação (CGSI) a fim de serem realizados estudos específicos de segurança da informação e comunicações e serem elaboradas propostas de segurança e defesa das infraestruturas críticas da informação. O grupo é composto por representantes dos ministérios e também por órgãos públicos e privados com interesse na área (MANDARINO JUNIOR, 2010).

Além do CGSI, também funcionam dentro da coordenação do GSI/PR:

- Grupos de Trabalho de Segurança das Infraestruturas Críticas, nas áreas de energia, telecomunicações, transportes, suprimento de água e finanças;
- Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação;
- Grupo Técnico de Segurança Cibernética; e
- Grupo Técnico de Criptografia.

O GSI/PR, com base na Lei nº 10.683 (2003), coordena a inteligência e atividades de segurança da informação. De tal modo assumiu um papel central na coordenação da estratégia e segurança cibernética nacional. O Departamento de Segurança da Informação e Comunicações (DSIC) e a Agência Brasileira de Inteligência (ABIN) são os seus subordinados que trabalham em favor da construção da estratégia de segurança cibernética.

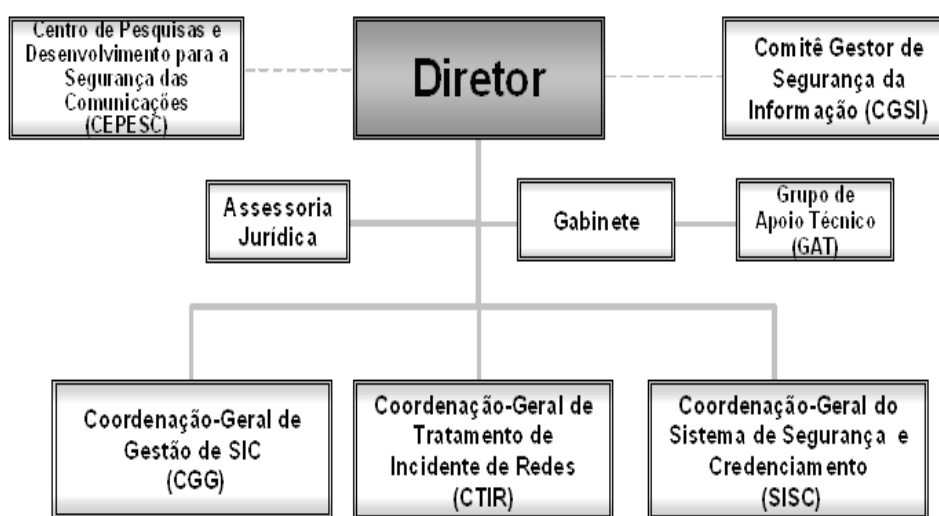
O DSIC tem por competência as seguintes atividades no processo de operacionalização das atividades relacionadas à SIC:

- regulamentar;
- avaliar tratados, acordos ou atos internacionais;

- coordenar o Sistema de Segurança e Credenciamento;
- definir requisitos metodológicos;
- planejar e coordenar gestão de assuntos, documentos e tecnologias sigilosos.

A estrutura do DSIC para o cumprimento das atividades listadas é a representada na Figura 21:

**Figura 21 - Organograma do DSIC.**



**Fonte: (DSIC, 2012)**

A ABIN trabalha na avaliação de ameaças internas e externas em tempo útil a fim de que seja colocado em prática os planos de defesa dos sistemas brasileiros. O Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC) é o órgão pertencente à ABIN que promove pesquisa científica e tecnológica para soluções em criptografias e algoritmos para o governo.

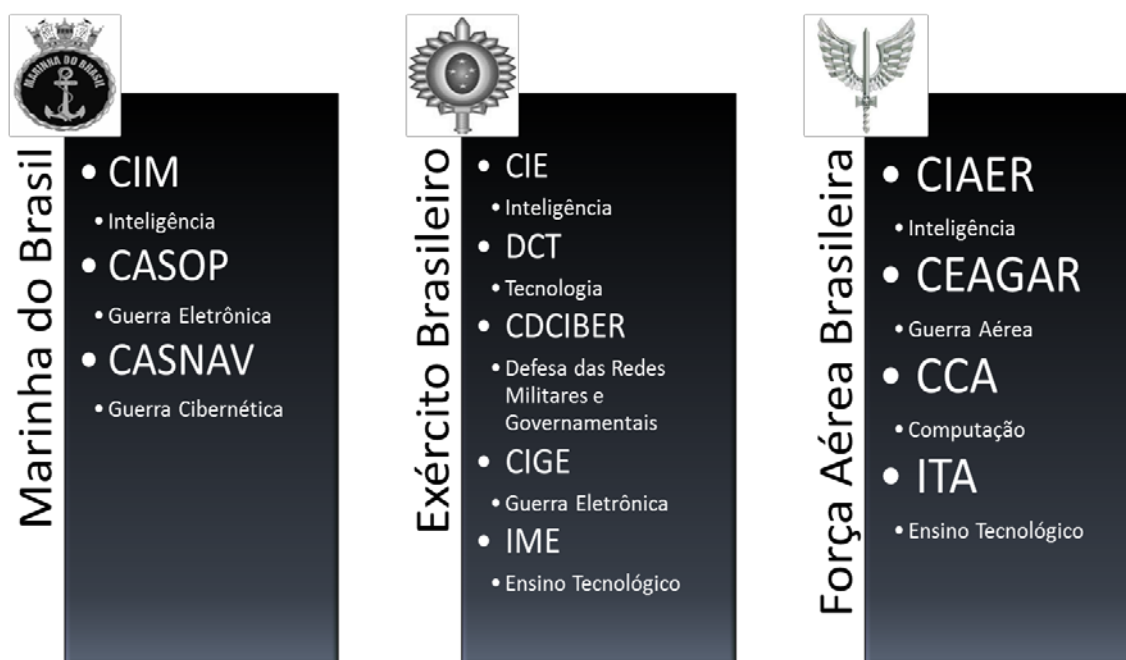
Outro órgão essencial da Presidência da República é a Casa Civil, cuja atuação no âmbito da defesa cibernética e segurança da informação ocorre por meio de uma autarquia federal a ela vinculada chamado Instituto Nacional de Tecnologia da Informação (ITI). Ele mantém a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, sendo a primeira autoridade da cadeia de certificação – AC Raiz. Tem como missão <sup>1</sup>:

<sup>1</sup> <http://www.iti.gov.br/twiki/bin/view/ITI/Apresentacao>

Atuar na inovação, regulação e provimento de soluções tecnológicas que garantam segurança, autenticidade, integridade, privacidade e validade jurídica de documentos e transações eletrônicas, respeitando o cidadão, a sociedade e o meio ambiente.

Uma vez que a manutenção da defesa cibernética envolve atividades relacionadas com a preservação da soberania nacional, conclui-se a responsabilidade de atuação do Ministério da Defesa por meio das Forças Armadas. A Marinha do Brasil, o Exército Brasileiro e a Força Aérea Brasileira compõem a estrutura do MD, aplicando suas tecnologias também para uso no mais recente campo de combate, o espaço cibernético.

**Figura 22 - Ministério da Defesa - Forças Armadas**



O EB tem destaque especial na condução das atividades cibernéticas do MD com o Centro de Defesa Cibernética (CDCiber) que, em linhas gerais, tem como objetivo (OLIVEIRA, 2011):

- expansão e aprimoramento da estrutura de segurança cibernética já existente;
- expansão e aprimoramento da estrutura de capacitação, adestramento e emprego operacional já existente, para atender, também, às necessidades do Setor Cibernético, incluindo, ainda, os assuntos relacionados ao tema nos

currículos dos estabelecimentos de ensino da Força;

- estabelecimento de uma estrutura de apoio tecnológico e de pesquisa cibernética;
- estabelecimento de uma estrutura de gestão de pessoal e de arcabouço documental (doutrina, em particular);
- estabelecimento de uma estrutura para atendimento das necessidades de inteligência voltadas para o setor; e
- formatação da estrutura e das missões do Centro de Defesa Cibernética do Exército, a partir do seu Núcleo já ativado.

O Ministério da Justiça (MJ) no exercício de suas atribuições pode se envolver com a segurança de defesa cibernética por meio do Departamento de Polícia Federal (DPF). Um exemplo seria sua atuação na repressão aos crimes praticados no espaço cibernético.

O Tribunal de Contas da União (TCU) dá atenção especial aos gestores públicos na questão da segurança da informação e da qualidade dos sistemas informatizados disponíveis ao público. O TCU possui a Secretaria de Fiscalização de Tecnologia da Informação (SEFTI) que é especializada na área com o objetivo de fiscalizar a gestão e o uso dos recursos de TI na APF. A SEFTI confecciona e divulga metodologias, manuais, notas técnicas e procedimentos para planejamento e execução de fiscalizações de TI realizando Diálogo Público de TI com a sociedade, Congresso Nacional e Gestores Públicos <sup>2</sup> (TCU, 2012).

### **3.3. Requisitos de Segurança da Informação Cibernética**

A segurança da informação é uma questão relevante para que os órgãos e entidades da APF cumpram suas missões institucionais e garantam um nível aceitável de risco para suas atividades cibernéticas, uma vez que todas as áreas críticas da administração pública dependem de TI.

Os requisitos de segurança da informação cibernética servem para conduzir um controle rigoroso dos serviços públicos <sup>2</sup> em que a administração diretamente, ou por meio de órgãos especializados, exerce vigilância, orientação e correção. Tal

---

<sup>2</sup> [http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia\\_informacao/sobre\\_sefti/historia](http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/sobre_sefti/historia)

controle interessa diretamente à população e é essencial para a subsistência da coletividade (ALEXANDRINO et al., 2011). Ele tem como objetivos:

- assegurar a eficácia, eficiência e economicidade na administração e aplicação dos recursos públicos.
- evitar desvios, perdas e desperdícios;
- garantir o cumprimento das normas técnicas, administrativas e legais;
- identificar erros, fraudes e respectivos agentes;
- preservar a integridade patrimonial; e
- propiciar informações para tomada de decisões.

Para isso, o Estado deve se valer de funções estratégicas de segurança cibernética, integrando ações nas áreas de (DSIC, 2010) a exemplo de:

- segurança das Infraestruturas Críticas;
- segurança da Informação e Comunicações;
- segurança Pública;
- inteligência;
- Defesa Nacional;
- Cooperação Internacional; e
- Construção de Marcos Legais.

O acórdão nº 1603 (2008) do TCU atribui ao GSIPR a incumbência de orientar os órgãos e entidades da APF no que diz respeito ao gerenciamento da segurança da informação, utilizando uma metodologia com base nos seguintes pressupostos (MANDARINO JUNIOR, 2010):

- busca de modelo adequado ao serviço público;
- construção das normas no CGSI;
- referência à ABNT 27001 (PDCA);
- considerar as boas práticas de mercado;
- visão de Segurança com cadeia de confiança;
- ultrapassar os limites de TI;

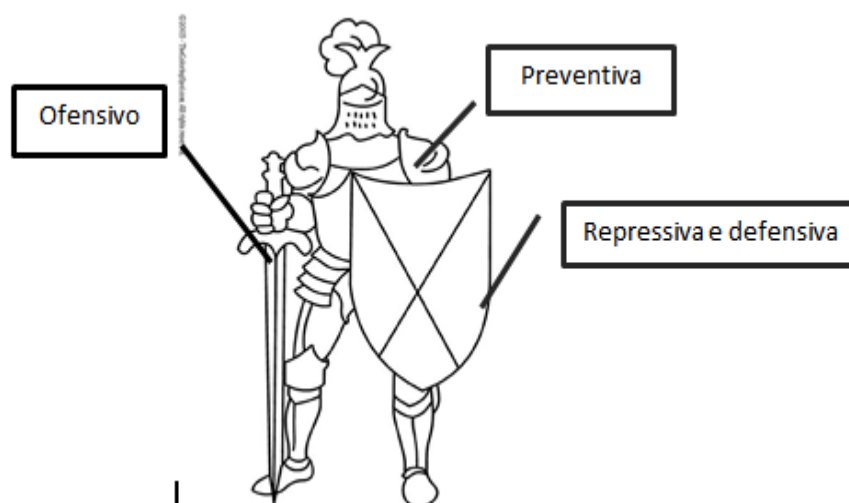
- ativos de informação (ambiente, pessoas, processos e tecnologias); e
- valorizar o comportamento (cultura de SIC).

O tratamento correto dado para a confidencialidade, a integridade, autenticidade e disponibilidade das informações de órgãos públicos é um pressuposto da segurança da informação e comunicações a ser cumprido por todos os órgãos e entidades da APF, uma vez que a prestação dos serviços aos cidadãos depende de tais requisitos (BRASIL, 2010).

### 3.4. Atuação para Segurança e Defesa Cibernética

As atuações das entidades do Governo podem ocorrer na forma de ações preventivas e repressivas para segurança cibernética, ou na forma de ações operacionais de defesa cibernética contra ataques relevantes (MANDARINO JUNIOR, 2010).

Figura 23 – Postura da Defesa Cibernética



Fonte : Adaptação de Fontenele, 2008, p. 35.

Para prevenção são adotadas medidas a fim de evitar que ataques cibernéticos sejam nocivos a infraestruturas críticas e sensíveis do Estado. Dessa forma, adotam-se métodos de gestão de risco e plano de contingência e continuidade. Nesse sentido, são gerenciados os equipamentos, os sistemas de comunicação e

softwares, e o investimento em capacitação dos técnicos e usuários dos sistemas. Trata a administração das redes de informação, com estudo e disseminação de medidas corretivas e boas práticas que estejam relacionadas com a segurança da informação (MANDARINO JUNIOR, 2010).

Para repressão, são realizados trabalhos de identificação e combate de condutas criminosas e sabotagens no espaço cibernético, incluindo-se ações em combate ao terrorismo cibernético, quando fora do contexto de Guerra declarada (MANDARINO, 2010).

A Tabela 5, a seguir, mostra resumidamente os órgãos em suas características institucionais quanto à participação na estratégia de defesa cibernética do país.

**Tabela 5 - Papéis na Segurança e Defesa Cibernética.**

Órgão	Papel			Ação		
	Estratégico	Tático	Operacional	Preventiva	Repressiva	Defensiva
CDN	X			X	X	X
CREDEN	X	X		X	X	X
CASA CIVL	X			X		
ITI		X		X		
GSI	X	X		X		
DSIC		X	X	X		
CTIR		X	X	X	X	
ABIN			X	X		X
MD	X					X
MB	X	X	X			X
EB	X	X	X			X
FAB	X	X	X			X
MJ		X	X	X	X	
PF		X	X	X	X	
TCU	X	X		X		

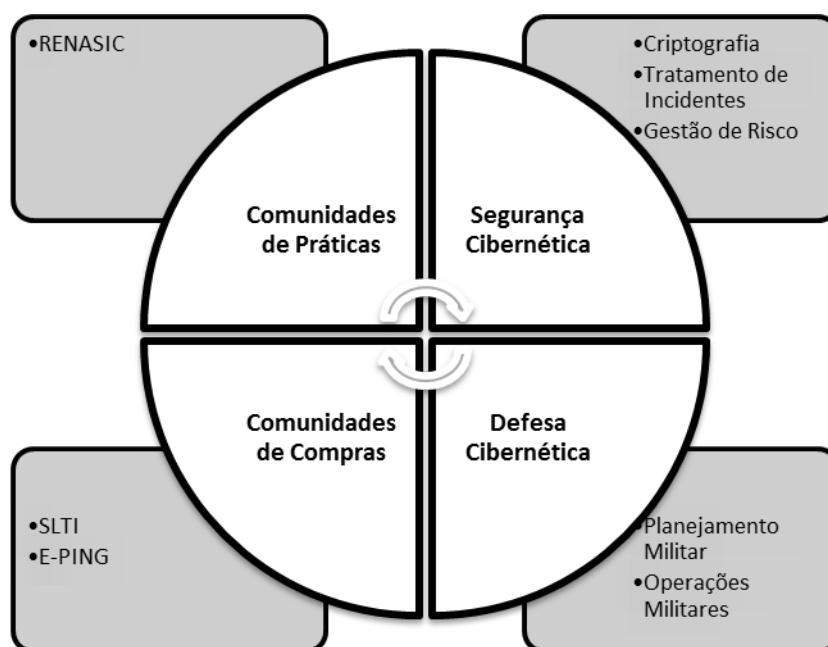
**Fonte: (MANDARINO JUNIOR, 2010, p. 119).**

A árdua tarefa de resguardar a segurança cibernética e assegurar a interação entre os órgãos da APF depende do fluxo das informações em situações de prevenção e de repressão de incidentes de segurança cibernética. Medidas que vão desde capacitação e troca de informações até a preparação para uma situação de guerra cibernética são tomadas de modo coordenado e coerente pelos órgãos envolvidos.

Exemplo disso é a demonstração feita na Figura 24 na qual a capacitação e a

troca de informações são representadas como Comunidades Práticas, tendo por referência a Rede Nacional de Segurança da Informação e Criptografia (RENASIC). O termo Comunidades de Compras refere-se a ações para exercer o poder de compra do estado, no qual são definidos os requisitos de segurança para proteção das informações do governo e dos equipamentos nos quais estas são armazenadas. Na Segurança Cibernética, são representadas as ações técnicas e operacionais para aplicação na APF. O último item, Defesa Cibernética, trata especificamente de guerra eletrônica e cibernética (MANDARINO JUNIOR, 2010).

**Figura 24 - Atuação em Segurança e Defesa Cibernética**



Fonte: (MANDARINO JUNIOR, 2010).

### 3.5. Normas, Regulamentos e Legislações

O conjunto de leis, decretos, portarias, instruções normativas, normas complementares e outros regulamentos de valor jurídico se fazem necessários para que se estabeleça a segurança da informação e comunicações na APF. Todas elas criam deveres por parte dos funcionários públicos e cidadãos inseridos nesse sistema. Por isso, a elaboração de um documento normativo é consequência de exaustivas discussões. Nesse sentido, para uma aplicação eficaz, deve ser claramente compreendido, ressaltado e monitorado regularmente no âmbito a que se destina. Deve ser rígido o suficiente para manter foco de evitar ações fraudulentas



em geral e ser submetidos a todos os níveis hierárquicos da organização.

A segurança da informação e comunicação na APF é pautada em seu arcabouço normativo para tratar da implantação e emprego de ferramentas e procedimentos, tais como:

- **Certificação digital nos sistemas estruturantes da APF:**

Documento eletrônico que se destina a registrar de forma única, exclusiva e intransferível a relação entre uma chave de criptografia e uma PJ, PF, máquina ou aplicação. por finalidade garantir a identidade das partes envolvidas em uma transação e proteger as informações sob a guarda do estado. Possui validade jurídica.

- **Infovia Brasília**

Infraestrutura de rede ótica metropolitana de comunicações, construída para fornecer, aos órgãos do Governo Federal situados em Brasília, um conjunto de serviços e funcionalidades em ambiente seguro, de alta performance e de alta disponibilidade. Tem por objetivo proporcionar uma significativa redução dos custos de comunicação e um ambiente capaz de servir de suporte à implementação das políticas públicas de Governo.

- **e-PING**

Arquitetura que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação no governo federal, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

- **NSIC – Núcleo de SIC do SISP**

O NSIC é um Fórum de Discussão dos Desafios da SIC para o SISP. Instituído pela Resolução SLTI nº 5, de 21 de dezembro de 2011. Objetivo principais: realizar estudos sobre SIC; elaborar e implementar normas de SIC; divulgar, implementar e monitorar boas práticas; propor capacitação de servidores em SIC.

Segundo Fontes (2006, p.135), são premissas básicas das normas:

- atender aos requisitos e às boas práticas de segurança e proteção da informação;
- atender aos requisitos éticos do negócio;
- ser adequado à realidade do negócio; e

- ser possível de ser cumprido pelos usuários.

As legislações de Segurança da Informação na APF aprovadas e publicadas estão disponíveis no portal do DSIC na internet<sup>3</sup>. São as seguintes:

**Tabela 6 - Legislações de Segurança da Informação na APF.**

<b>Legislação</b>	<b>Assunto</b>
<b>Decreto Nº 3.505 (PRESIDÊNCIA, 2002)</b>	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
<b>Decreto Nº 4.553 (PRESIDÊNCIA, 2002)</b>	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
<b>Instrução Normativa GSI/PR Nº1 (GSIPR, 2008b)</b>	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
<b>Norma Complementar 01/IN01/DSIC/GSIPR (GSIPR, 2008c)</b>	Atividade de Normatização
<b>Norma Complementar 02/IN01/DSIC/GSIPR (GSIPR, 2008d)</b>	Metodologia de Gestão de Segurança da Informação e Comunicações.
<b>Norma Complementar 03/IN01/DSIC/GSIPR (GSIPR, 2009a)</b>	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.
<b>Norma Complementar 04/IN01/DSIC/GSIPR (GSIPR, 2009b)</b>	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.
<b>Norma Complementar 05/IN01/DSIC/GSIPR (GSIPR, 2009c)</b>	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.
<b>Norma Complementar 06/IN01/DSIC/GSIPR (GSIPR, 2009d)</b>	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
<b>Norma Complementar 07/IN01/DSIC/GSIPR (GSIPR, 2010a)</b>	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
<b>Norma Complementar 08/IN01/DSIC/GSIPR (GSIPR, 2010b)</b>	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.
<b>Norma Complementar 09/IN01/DSIC/GSIPR (GSIPR, 2010c)</b>	Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta.

Anexo A, anexo B e anexo C deste trabalho apresentam os Dispositivos Legais e Legislações Específicas de caráter federal bem como alguns dos projetos de lei

<sup>3</sup> <http://dsic.planalto.gov.br>

relacionados à segurança da informação.

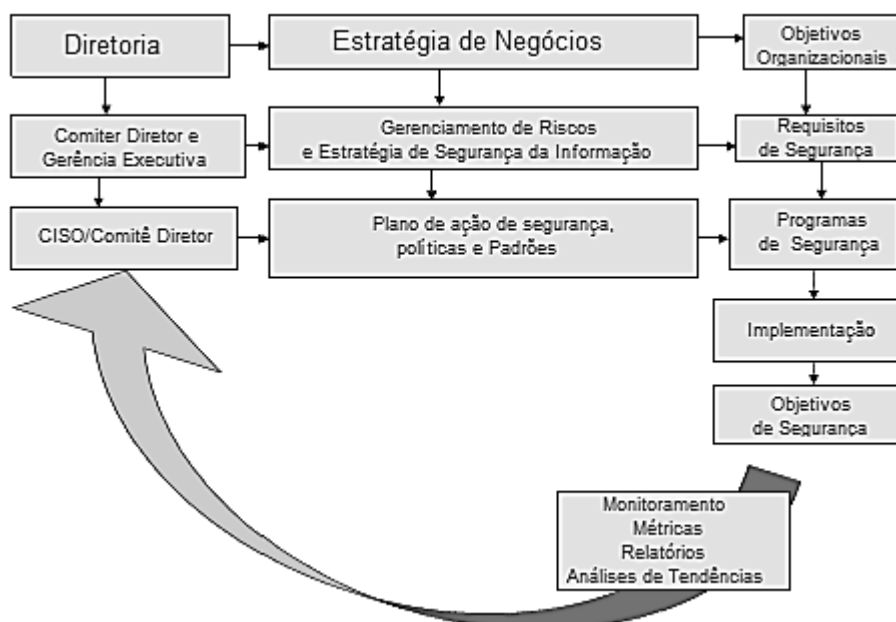
## 4. PROPOSTAS DE GOVERNANÇA PARA O CENÁRIO CIBERNÉTICO BRASILEIRO

A Governança da Segurança da Informação permite o direcionamento da Gestão da Segurança da Informação para cuidar do espaço cibernético, protegendo as comunicações, os bancos de dados da administração pública, e especialmente, o resguardo das infraestruturas críticas.

A implantação do conjunto de boas práticas em segurança da informação tem por objetivo garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações em meio ao aumento das ameaças e tentativas de ataques contra as redes de instituições estratégicas do governo.

Os envolvidos na estratégia de segurança devem trabalhar para desenvolver a estratégia de segurança alinhada com o objetivo institucional, de modo que da Diretoria partam as diretrizes estratégicas e sigam conforme a Figura 25.

**Figura 25 - A Governança de Segurança da Informação.**



Fonte: (ITGI, 2006).

O retorno obtido para a organização depende das metas estabelecidas dentro da Governança de Segurança da Informação para cada um dos objetivos conforme

é apresentado na Tabela 7.

**Tabela 7 - Objetivos da GSI.**

<b>Objetivo</b>	<b>Meta</b>
<b>Alinhamento Estratégico</b>	Alinhar as ações de Segurança da Informação com os objetivos estratégicos do negócio.
<b>Gestão de Riscos</b>	Gerenciar riscos e reduzir o impacto nos ativos de informação para níveis aceitáveis.
<b>Gestão de Recursos</b>	Direcionar o uso do conhecimento e de infraestrutura de segurança de forma eficiente e eficaz.
<b>Gestão de Desempenho</b>	Medir e monitorar os processos de SI. Reportar os resultados para atingir os objetivos do negócio.
<b>Entrega de Valor</b>	Otimizar os investimentos em SI que oferecem suporte aos objetivos organizacionais.

Na época da criação do Grupo Técnico de Segurança Cibernética – GT SEG CIBER, em 2009, o diretor do DSIC, Raphael Mandarino Jr., deu o seguinte depoimento no site Convergência Digital<sup>4</sup> (2009):

Estamos estudando como proteger a infraestrutura crítica do país, aquilo que se parar traz consequências graves para o cidadão como, por exemplo, as telecomunicações, água, energia, transporte. Temos que lembrar que a estrutura física da informação permeia todas as outras.

Propostas de Governança de Segurança da Informação para o âmbito cibernético da APF são importantes para melhorar o nível de maturidade e proporcionar uma melhor gestão de riscos com base no referencial teórico dos modelos mais consagrados.

#### **4.1. Aplicabilidade do COBIT**

O COBIT é aplicável dentro de uma organização, relacionado a diferentes pontos de vista (FERNANDES et al., 2012), por exemplo:

- Gestão Executiva – Fornece orientação acerca da obtenção de retorno sobre investimentos em TI de acordo com os riscos inerentes ao ambiente de TI.
- Gestão do Negócio – Auxilia a obter maiores garantias sobre o gerenciamento dos serviços de TI.
- Gestão de TI – Auxilia a prover serviços de TI adequados a suportar a

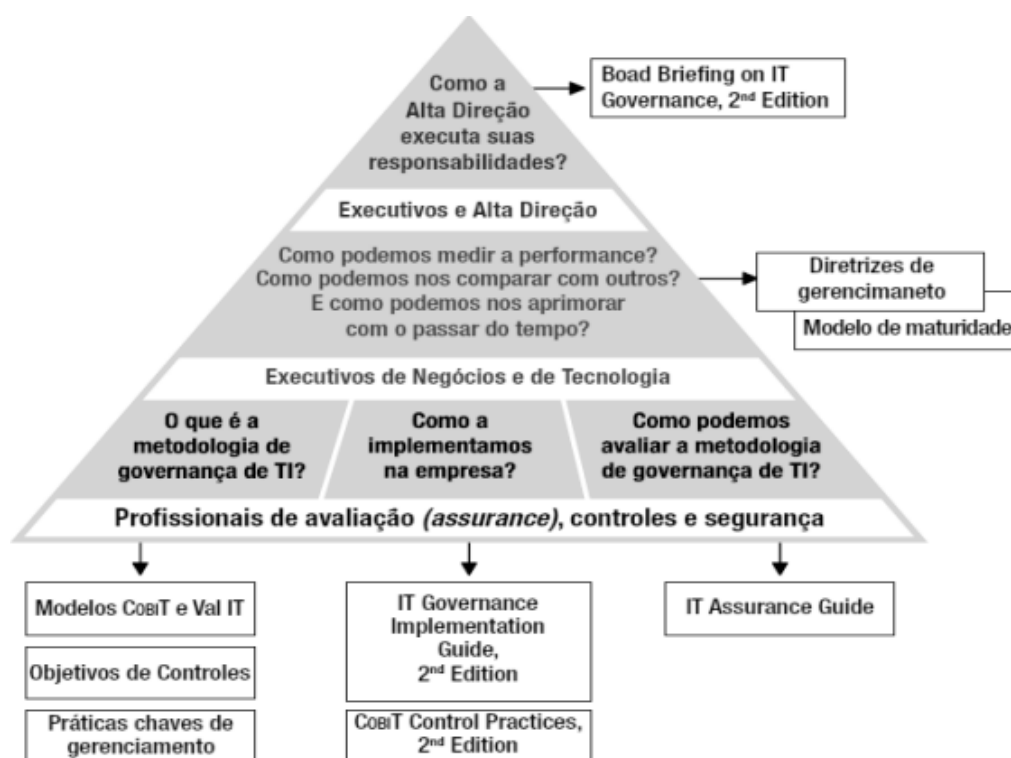
<sup>4</sup> <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=20226&sid=11>

estratégia do negócio, de forma controlada e gerenciada.

- Audidores – Fornece o embasamento para suas conclusões e orientação para a gestão dos controles internos.

Especificamente sobre Governança em segurança da Informação, o COBIT possibilita a inserção de métricas que propiciam o acompanhamento dos requisitos de alinhamento estratégico, *compliance* e segurança da informação, de modo a fornecer uma visão estratégica de segurança no nível mais alto da organização. A sua estrutura em três níveis dá suporte aos profissionais que atuam nos aspectos citados anteriormente, conforme indicado na Figura 26 (ITGI, 2006).

Figura 26 - Conteúdo do COBIT.



Fonte: (ISACA, 2007)

Os processos do COBIT contemplam assuntos de segurança. Entretanto, dentre os 34 vistos anteriormente, destacam-se os quatro que incidem diretamente na segurança da informação por seus objetivos, são eles:

- PO 6 - Comunicar objetivos e direcionamentos gerenciais;
- PO 9 – Avaliar e gerenciar os Riscos de TI;
- DS 4 – Garantir a continuidade dos Serviços;
- DS 5 – Garantir a Segurança dos Sistemas.

O COBIT em seus modelos fornece suporte para implementação de controles internos, conforme as leis e regulamentações. Processos de auditoria, monitoração, definição de níveis de maturidade são úteis para o cumprimento dos objetivos de segurança da informação por parte dos gestores das organizações.

Para o COBIT (ISACA, 2007), todas as mudanças, manutenções e aplicação de patches de correção para a infraestrutura e aplicações de tecnologia devem ser formalmente gerenciadas e controladas. Isso evita que a instabilidade ou integridade incida em impactos na segurança. O gerenciamento de mudança é abordado no processo 6 – Gerência de Mudanças, do domínio Aquisição e Implementação.

No que se refere à gestão dos riscos, o COBIT exige o comprometimento da alta direção executiva da organização, compreensão de quais riscos são aceitáveis de acordo com os requisitos normativos e quais são significativos, atribuindo responsabilidades para a correta administração deles. A gestão de riscos pode ser qualificada segundo o modelo de maturidade (ISACA, 2007) derivado do *Capability Maturity Model* – CMM. Com base nesses modelos de maturidade, a situação atual pode ser mapeada, com a realização de *benchmarking*, avaliada conforme os padrões internacionais e monitorada de acordo com a estratégia da organização (FERNANDES et al., 2012).

Vale mencionar que o COBIT pode ser aplicado tanto em pequenas como em grandes organizações de TI, desde que tenha definidos seus objetivos de negócio e estratégias relacionadas à TI (FERNANDES et al., 2012).

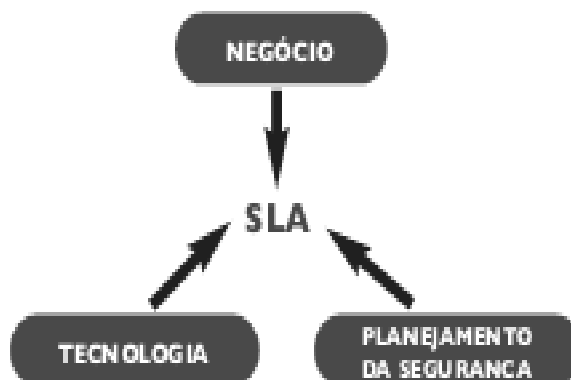
## 4.2. Aplicabilidade do ITIL

No Núcleo ITIL, na publicação desenho de serviço, consta orientação quanto ao gerenciamento da segurança da Informação, abordando processos relacionados à garantia dos critérios de confidencialidade, integridade e disponibilidade de dados, bem como a segurança dos componentes de hardware e software, documentações e procedimentos. Dessa forma, busca com que o gerenciamento da segurança da informação seja efetivo, mantendo alinhadas a segurança de TI e a segurança do negócio (FERNANDES; ABREU, 2008).

As práticas da ITIL prezam por uma forte abordagem de gestão, adaptável às características de cada organização, com ênfase nos aspectos tecnológicos e na sua integração com os requisitos do negócio (FERNANDES et al., 2012).

ITIL dá importância à Gestão de Segurança da Informação, considerando o Gerenciamento de Nível de Serviço de TI, ou ANS e conhecido também como SLA, entre processos de negócio e os da TI (INFOSEC COUNCIL, 2005).

Figura 27 - Gestão da Segurança no ITIL.



De um modo geral, os itens que podem ser colocados para melhoria da segurança recomendados pelo ITIL são (INFOSEC COUNCIL, 2005):

- Catálogo de Serviços: a TI deve publicar na Organização um descritivo de seus serviços, com as respectivas condições, que atendem a cada requisito do Negócio;
- OLA's (Operational Level Agreement): deve ser estabelecido; é um SLA



mais “enxuto”, mas prevendo integralmente os serviços e suas condições, inclusive custos internos;

- UC’s – Underpinning Contracts: são aqueles contratos estabelecidos com provedores externos, nos quais devem ser previstas todas as condições, incluindo bônus, penalidades, condições de saída, etc.;
- Banco de Dados dos ativos existentes e suas configurações atualizadas, incluindo software, hardware, documentação atualizada, procedimentos e classificação quanto à Segurança;
- Criação de um Service Desk como ponto focal de contato para todos os Usuários de TI; é a área “dona” de todos os incidentes e seu foco é a continuidade de serviço e manutenção do SLA; incluem-se aí os incidentes de Segurança;
- Gestão de Problemas: nessa área são estudados os incidentes, determinando sua relação, causas e medidas para evitá-los; essa abordagem permite detectar “brechas” de Segurança e deve prever forte documentação dos incidentes e soluções;
- Gestão de Mudanças: coordenam todas as mudanças em infraestrutura de TI, apoia-se na documentação dos incidentes e é responsável pela mudança;

O processo de Gerenciamento de Continuidade garante a continuidade dos serviços de TI que suportam os processos de negócio da organização de acordo com o nível de maturidade ao qual a organização está submetida. Estando comprometida a operação de um sistema, o gerenciamento deve proporcionar a recuperação em menor tempo possível dentro das prioridades. O passo inicial é determinar todos os processos críticos das áreas de TI base para o negócio da organização e as medidas para evitar a interrupção da continuidade dos serviços de TI (MAGALHAES; PINHEIRO, 2007).

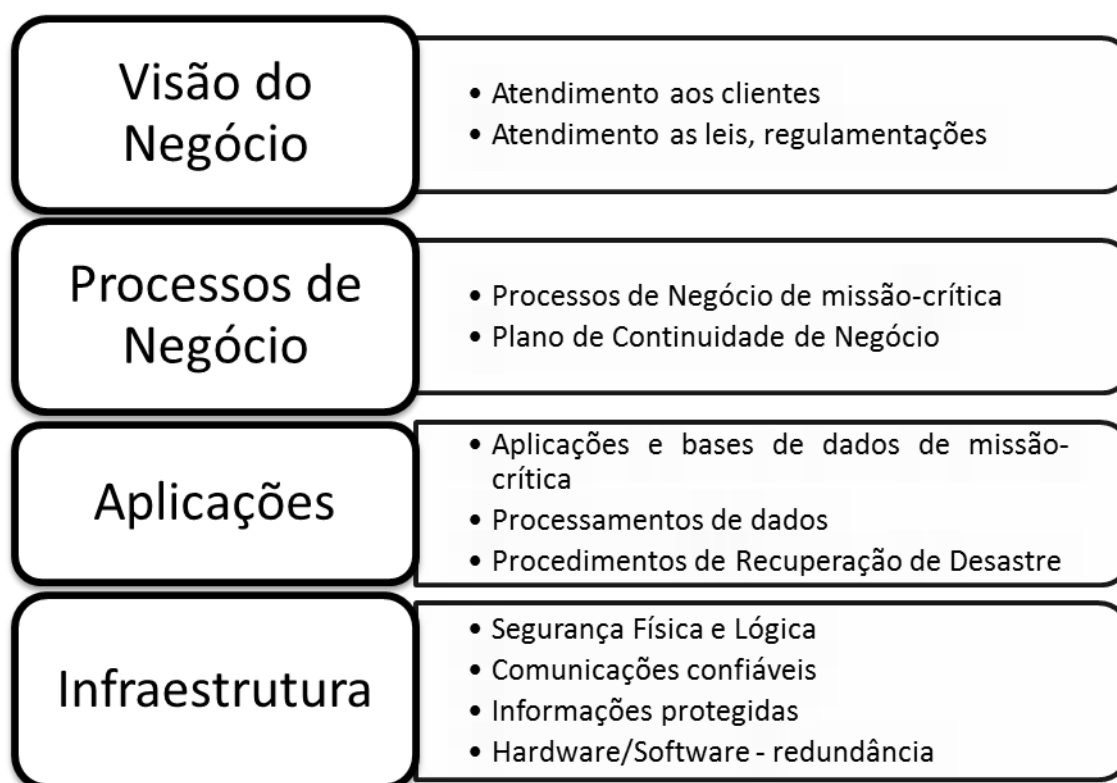
Os principais objetivos que devem ser atingidos pelo PCN são (MAGALHAES; PINHEIRO, 2007):

- garantir a segurança dos empregados e visitantes;
- minimizar danos imediatos e perdas em uma situação de emergência;

- assegurar a restauração das atividades, das instalações e dos equipamentos o mais rápido possível;
- assegurar a rápida ativação dos processos de negócio críticos;
- fornecer conscientização e treinamento para as pessoas-chave encarregadas de tal atividade.

O PCN é imprescindível porque a interrupção dos processos de negócios representa risco de prejuízos financeiros e de imagem. A Figura 28 indica os pontos mais críticos para uma organização, nos seus domínios:

**Figura 28 – Pontos mais críticos para o negócio.**

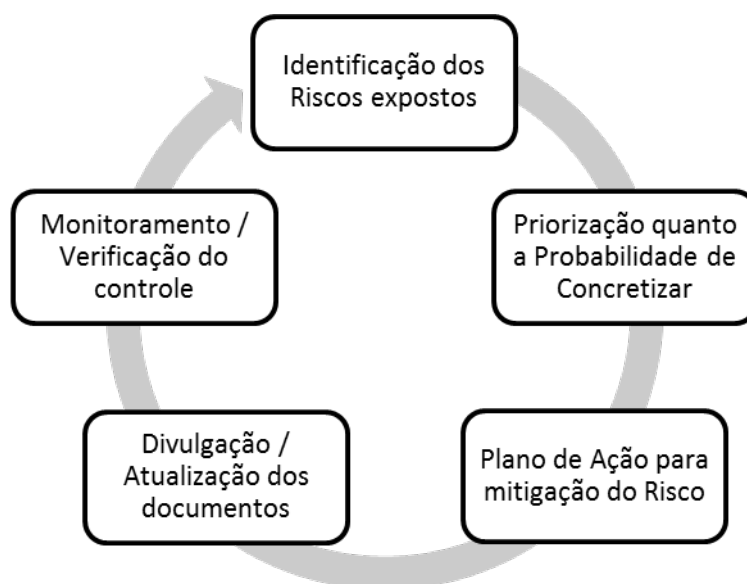


Os riscos que a organização está exposta precisam ser identificados com o propósito de estabelecer os requisitos de disponibilidade dos serviços de TI e justificar os requisitos com os custos relacionados para tornar possível investimento em sua atenuação e proceder à elaboração do PCN (MAGALHAES; PINHEIRO, 2007).

A fim de que as organizações se previnam diante da possibilidade de ocorrer algum fato temível, devem ser colocadas em prática as 5 atividades de

Gerenciamento de Riscos para o negócio (Figura 29) com o objetivo de controlar, identificar e analisar todos os riscos. A aplicação desse processo torna possível maior adaptação às circunstâncias e competitividade na execução de seus processos críticos pela organização.

**Figura 29 – Processo de Gerenciamento dos Riscos.**

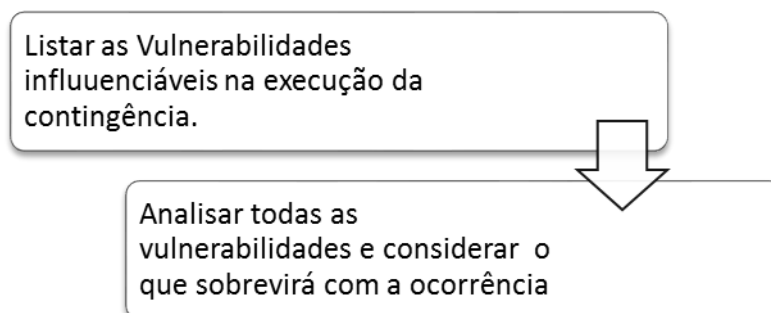


Fonte: adaptado de (MAGALHAES; PINHEIRO, 2007, p. 412).

Para um estudo pormenorizado das vulnerabilidades, a ITIL prevê 2 passos (

Figura 30) a serem adotados, nos quais devem ser aplicados uma escala de 1 a 5 em ordem crescente de probabilidade, considerando os custos para: substituir, configuração temporária e de reparação (MAGALHAES; PINHEIRO, 2007).

**Figura 30 – passos para análise das vulnerabilidades**



O exame dos impactos que podem afetar a organização pode ser quantificado e qualificado com uso do ITIL. Possibilita a realização de uma análise crítica dos processos de negócios quanto às prioridades de recuperação e interdependências a fim de que o reestabelecimento dos serviços ocorra dentro do prazo instituído.

Nesse sentido, é considerado fundamental nessa etapa:

- identificar os eventos que podem causar interrupções nos processos de negócios;
- avaliar os riscos e assim determinar o impacto das interrupções;
- elaborar um plano estratégico que proporcione ou ajude a proporcionar a continuidade do negócio.

As categorias do impacto (Tabela 8 – categorias de impactoTabela 8) são utilizadas para uma avaliação quantitativa de acordo com os riscos e as áreas em que melhorias não podem deixar de ocorrer.

**Tabela 8 – categorias de impacto.**

<b>Nível</b>	<b>Definição</b>
<b>Alto</b>	<ul style="list-style-type: none"> <li>• Perda significativa dos principais ativos e recursos;</li> <li>• Perda da reputação, imagem e credibilidade;</li> <li>• Impossibilidade de continuar com as atividades de negócio.</li> </ul>
<b>Médio</b>	<ul style="list-style-type: none"> <li>• Perda dos principais ativos e recursos;</li> <li>• Perda da reputação, imagem e credibilidade.</li> </ul>
<b>Baixo</b>	<ul style="list-style-type: none"> <li>• Perda de alguns dos principais ativos e recursos;</li> <li>• Perda da reputação da imagem e credibilidade.</li> </ul>

Fonte: (MAGALHAES; PINHEIRO, 2007)

O processo de Gerenciamento de Continuidade envolve toda a organização, principalmente a alta administração. Os 7 pontos que fazem parte do PCN são: planejamento, pessoas, processos, premissas, provedores, perfil da organização e desempenho.

### **4.3. Aplicabilidade da ABNT NBR ISO/IEC ISO 17799:2005**

Por se tratar de uma norma de prática para gestão da segurança da informação, essa norma se aplica diretamente a organizações que utilizam a TI para alcançar os objetivos do negócio, fazendo com que seja praticamente obrigatória para garantir a proteção dos ativos e significando um diferencial competitivo. Ela proporciona prevenção para perdas em caso de vir a ocorrer algum risco de segurança da informação (FERNANDES et al., 2012).

A aplicação de um sistema de gerenciamento de segurança da informação pode ser realizada em etapas cujo enfoque principal seja os aspectos críticos de segurança cibernética, que nas organizações podem ocorrer na parte física ou lógica. Deve ser considerada como um projeto de longa ou média duração, de acordo com a organização, e requer investimentos direcionados a esse fim.

O Sistema de Gestão de segurança da Informação definido na norma fornece a orientação para gerenciamento dos riscos de segurança da informação. Ele indica o que deve ser feito sem ser específico, bem como a forma com que deve ser aplicada. Para tanto, Sêmola (2003) indica um teste de conformidade superficial; ou seja, um diagnóstico para auxílio na percepção do nível de aderência da organização com relação às recomendações de Segurança da Informação da norma ISO 17799. Esse teste pode ser visualizado no Anexo F.

A norma ISO/IEC 17799:2005 é aplicada por Entidades Fiscalizadoras Superiores, órgãos de governo, empresas públicas e privadas nacionais e internacionais para segurança da informação por meio de acordos e decisões (TCU, 2008). A análise e a avaliação feitas com a norma permitem que a organização identifique seus requisitos em segurança da informação, além de legislações vigentes, estatutos, regulamentações e cláusulas contratuais para apoiar e estabelecer as operações da organização.

A ISO/IEC 17799:2005 prevê que a Política de Segurança da Informação deva ser alvo de comprometimento da alta direção e deva ser comunicada a todos os funcionários. Trazendo em seu conteúdo, dentre outras, as seguintes declarações:

- conceituação da segurança da informação, as metas globais, escopo e importância da segurança como mecanismo que habilita o compartilhamento de informações;
- declaração do comprometimento da direção, apoiando as metas e princípios

- da segurança, alinhado com os objetivos estratégicos do negócio;
- estrutura para estabelecer os objetivos de controle e os controles, incluindo a análise, avaliação e gerenciamento de riscos.
  - breve explanação das políticas, princípios, normas e requisitos de conformidade da segurança da informação específico para a organização;
  - definição de responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro de incidentes de segurança; e
  - referências à documentação que possam apoiar a política.

A organização da Segurança da Informação, segundo a norma ISO/IEC 17799:2005, indica que:

- uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização;
- a direção aprove a política de segurança da informação, atribua as funções da segurança, coordene e analise criticamente a implementação da segurança da informação por toda a organização;
- se necessário, uma consultoria especializada em segurança da informação seja estabelecida e disponibilizada dentro da organização;
- contatos com especialistas ou grupos de segurança da informação externos, incluindo autoridades relevantes, sejam feitos para se manter atualizado com as tendências do mercado, normas de monitoração e métodos de avaliação, além de fornecer apoio adequado, quando estiver tratando de incidentes de segurança da informação;
- um enfoque multidisciplinar na segurança da informação seja incentivado.

Também, de acordo com a norma ISO/IEC 17799:2005, o objetivo das Partes Externas é manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas. Assim, convém que:

- a segurança dos recursos de processamento da informação e da informação da organização não seja reduzida pela introdução de produtos ou serviços

oriundos de partes externas;

- qualquer acesso aos recursos de processamento da informação da organização e ao processamento e comunicação da informação por partes externas seja controlado;
- seja feita uma análise/avaliação dos riscos envolvidos para determinar as possíveis implicações na segurança e os controles necessários. Onde existir uma necessidade de negócio para trabalhar com partes externas, que possa requerer acesso aos recursos de processamento da informação e à informação da organização, ou na obtenção e fornecimento de um produto e serviço de uma parte externa ou para ela;
- controles sejam acordados e definidos por meio de um acordo com a parte externa.

No que se refere à gestão de riscos, a ISO/IEC 17799:2005 prevê atividades coordenadas para direcionar e controlar a organização, fazendo com que haja análise, avaliação, tratamento, aceitação e comunicação dos riscos.

Para cada risco identificado, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco deve ser tomada. As possíveis opções são:

- aplicar controles apropriados para reduzir os riscos;
- conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para a aceitação de risco;
- evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;
- transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Para os riscos no qual a decisão de tratamento seja a de aplicar os controles apropriados, convém que esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos. A princípio, esses controles devem assegurar que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

- os requisitos e restrições de legislações e regulamentações nacionais e internacionais;
- os objetivos organizacionais;
- os requisitos e restrições operacionais;
- custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da organização; e
- a necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Os objetivos de controles apropriados para uma organização pública para proteção cibernética devem ser selecionados de acordo com a análise dos riscos a que a organização pública possa estar sujeita. Isso determinará a sua real necessidade, viabilidade, relação custo benefício para, a partir de então, os controles serem implantados.

#### **4.4. Aplicabilidade do PMBOK**

O PMBOK pode ser usado para definir os procedimentos a serem adotados em um projeto de implantação da segurança da informação, destinado a controlar o acesso a informações críticas contra modificação, destruição e utilização indevida ou não autorizada. A sua formalização na Administração Pública Federal incide em padronização da documentação dos procedimentos, ferramentas e técnicas utilizadas, e principalmente na criação de indicadores para monitoramento. A aplicação dos PMBOK deve estar adaptada e integrada aos princípios da Governança de TI em todas as suas áreas do conhecimento (BRITO, 2009).

De acordo com Brito (2009):

As áreas de conhecimento, as métricas de avaliação e principalmente a documentação gerada pelas lições aprendidas no projeto implementação do SGSIC são fatores críticos de sucesso para a criação da cultura de Gestão da Segurança da Informação e Comunicação.

Para a organização pública, em suas ações em favor da defesa cibernética, é



necessário que se faça uso do ciclo PDCA e se elabore formulários específicos para administrar a complexidade e controlar os riscos. Somado ao PMBOK, o PDCA dá o direcionamento necessário dentro de uma visão mais ampla (BRITO, 2009). O PMBOK também pode ser aplicado total ou parcialmente, fazendo uso de ferramentas de gerenciamento de projetos existentes. Tudo isso significa dar a consistência necessária, pois deverão ser feitas adaptações em função do tipo, porte e riscos da organização (FERNANDES et al., 2012).

Normalmente há consideráveis resistências dentro das organizações na aplicação de metodologias de gerenciamento de projetos. Um dos fatores mais importantes para se alcançar o objetivo é um grande comprometimento da alta administração e gerentes de TI, não só os relacionados com a segurança cibernética especificamente.

#### **4.5. Aplicação da Norma ISO 17799 com os Modelos COBIT e ITIL**

A relação entre a norma ISO 17799 com os modelos COBIT e ITIL aplicados ao tema da segurança cibernética contribui de modo mais eficaz na diminuição dos riscos relacionados com o uso da tecnologia da informação no espaço cibernético e para a análise dos indicadores.

A Governança de segurança da Informação de uma organização pode tirar proveito em níveis organizacional, tático e estratégico dos objetivos de controle abordados pelo modelo COBIT e pela norma ISO 17799, bem como os referenciados pelos processos abordados pelo modelo ITIL, conforme indicado no ANEXO Tabela 13 (BERNARDES et al., 2005).

Para a implementação da defesa cibernética na APF dentro dos requisitos deste trabalho, a Tabela 9 propõe a utilização do COBIT e ITIL, tendo por base a norma ISO 17799 que detalha o gerenciamento de segurança computacional. O COBIT terá, para os serviços de tecnologia oferecidos pela organização, seus controles em alto nível adaptados às práticas de segurança computacional, dando uma maior abrangência à ISO 17799 que possui seus controles de forma mais detalhada. Nisso deve ainda ser incluídas a avaliação do nível de maturidade e os processos de melhoria contínua para cada um dos controles da ISO (BERNARDES et al., 2005).

Posteriormente ao fornecimento dos controles pelo COBIT e ISO 17799, a ITIL detalha o que deverá ser feito em nível operacional e tático, e quem será o seu responsável. No nível estratégico da organização, é realizada a análise de risco nas situações em que serão definidos os requisitos a serem implementados, o modelo de maturidade estipulado e as necessidades de investimentos na execução do planejamento (BERNARDES et al., 2005).

**Tabela 9 - Correlação da ISO 17799 com os modelos COBIT e ITIL como proposta para um modelo de Governança da Segurança da Informação.**

	Operacional	Tático	Estratégico
Controles	- ISO 17799 - COBIT: Entrega e Suporte - COBIT: Aquisição e Implementação	- ISO 17799 - COBIT: Entrega e Suporte	- ISO 1799 - Análise de Risco - COBIT: Auditoria - COBIT: Monitoramento -COBIT: Planej. e Organização
Pessoas	-ITIL: Suporte a Serviços (adaptado)	- ITIL: Entrega de Serviços (expandido)	- COBIT: Auditoria - COBIT: Monitoramento
Processos	-ITIL: Suporte a Serviços (adaptado)	- ITIL: Entrega de Serviços (expandido)	- COBIT: Auditoria - COBIT: Monitoramento
Tecnologia	-Ferramentas de Workflow -Ferramentas de Gerenciamento (coleta de dados) -Data Warehouse	- Ferramentas de Workflow - Ferramentas de Gerenciamento (coleta de dados) - Data Warehouse - Ferramentas para testes de vulnerabilidade e penetração - Ferramentas para análise de logs	- Ferramentas automatizadas para análise de Risco. -Ferramentas automatizadas para a extração de conhecimento

Fonte: (BERNARDES et al., 2005).

## 5. CONCLUSÃO

A proposta deste trabalho referente à Governança de TI para segurança cibernética da Administração Pública Federal atinge principalmente a estrutura de decisão dos sistemas de informações gerenciais. Dessa forma, ela pode ser aplicada pela alta gerência dessas organizações, inserindo-se na realidade de suas organizações.

Sabe-se que há dificuldades para tomada de decisões relacionadas a negócios e ao gerenciamento de segurança cibernética, quando se trabalha com grandes volumes de dados. Nesse sentido, a motivação para utilização desta proposta

consiste no que pode ser extraído com mais relevância sobre as principais referências da área de Governança de TI.

Os conceitos apresentados no levantamento bibliográfico subsidiaram a construção do contexto que permite a análise holística que dá respaldo para compreender a Gestão de Segurança da Informação nos Órgãos da APF e as propostas desenvolvidas neste trabalho para aplicação da Governança no cenário cibernético brasileiro.

Antes das propostas apresentadas, foi feito um mapeamento da Gestão da Segurança da informação na APF, levando-se em consideração as dimensões relevantes para o alinhamento estratégico entre a segurança cibernética com o negócio da organização pública. Devido a essa abrangência, foram elencados os controles, processos, pessoas e tecnologias de acordo com os níveis de decisão: estratégico, tático e operacional. Nesse mapeamento, através dos levantamentos realizados pelo Tribunal de Contas da União, foi possível concluir que o país carece de uma apropriada gestão estratégica do espaço cibernético e da necessidade de segurança desse espaço cada vez mais relacionado com a segurança da própria Nação.

As melhores práticas dos principais modelos de Governança de TI por serem desenvolvidos por especialistas, testados e implementados em grande escala por organizações ao redor do mundo facilitaram a utilização e adaptação para os órgãos da APF, pautando-se na segurança cibernética. O uso de modelos bem conhecidos também permitiu o uso de uma linguagem homogênea e padronizada de fácil entendimento pela organização, a fim de facilitar a adoção das medidas por estarem disponíveis ao conhecimento público.

Com o aprofundamento dos estudos, verificou-se que a segurança cibernética é discutida amplamente pelos principais governos mundiais e que há uma necessidade urgente e constante da construção de uma doutrina que garanta uma segurança efetiva das infraestruturas críticas nacionais. Com isso, foram reconhecidas a dificuldade e a grandeza da tarefa de estabelecer uma Governança com esse propósito.

Dessa forma, ressalta-se a necessidade de contribuir colaborativamente por meio de propostas com a visão técnico-estratégica que vem sendo adotada pelo Governo com o apoio de diversos especialistas de diferentes órgãos da APF e

efetivada na missão do GSIPR.

Para apoiar a alta administração do Governo, foram adaptados os modelos COBIT, ITIL, NBR ISO/IEC 17799:2005 e PMBOK para as aplicabilidades propostas. Para que se alcance a Governança de Segurança da Informação, a combinação desses modelos permitiu potencializar as medidas que elas oferecem, a fim de identificar as seguintes indagações: o que, quem, como e com que recurso.

Com tudo isso, pretendeu-se colaborar com o fortalecimento da segurança da informação, que nos permitiu idealizar uma Administração Pública com processos de negócios mais eficazes e eficientes, em que os recursos públicos estejam protegidos de desperdícios, desvios, fraudes e ataques cibernéticos.

## REFERÊNCIAS

ALBERTIN, Rosa Maria de Moura; ALBERTIN, Alberto Luiz. **Estratégias de governança de tecnologia da informação: Estrutura e Práticas**. Rio de Janeiro: Elsevier, 2010.

ALEXANDRINO, Marcelo; PAULO, Vicente. **Direito administrativo descomplicado**. 19. ed. São Paulo: Método, 2011.

ANONIMO. 2001. **Segurança Máxima**. 3ª Ed. Rio de Janeiro: Campus, 2001.

BERNARDES, Mauro Cesar; MOREIRA, Edson do Santos. **Um modelo para Inclusão da Governança da Segurança da Informação no Escopo da Governança Organizacional**. São Paulo: Instituto de Ciências Matemáticas e de Computação - ICMC, USP, 2005.

BERNARDES, Mauro Cesar; MOREIRA, Edson dos Santos. **Artigo científico: um modelo para inclusão da governança da segurança da informação no escopo da governança organizacional**, v.1, n.1, p. 1-10, out. 2005.  
Disponível em: <<ftp://linorg.cirp.usp.br/pub1/SSI/SSI2005/artigos.html>>. Acesso em: 28 maio 2012.

BRANCO JÚNIOR, Paulo Ribeiro. **Agência de Inteligência e Guerra Cibernética: uma proposta para defesa nacional**. Brasília: Monografia (Especialização em Inteligência Estratégica) - FALBE, 2005.

BRASIL - Presidência da República, GSI/PR. de 13 de junho de 2008. **Instrução Normativa GSI/PR n. 1**. Brasília: s.n., de 13 de junho de 2008.

BRASIL, Ministério da Defesa. **Glossário das Forças Armadas** - MD35-G-01. 19 de Julho de 2008. Apresenta definições de termos comuns às Forças Armadas.

BRASIL, Tribunal de Contas da União (TCU). **Levantamento de governança de TI**. TCU. Brasília: TCU, 2010. p. 49. Relator Ministro Aroldo Cedraz – Disponível em: <[www.tcu.gov.br/fiscalizacaoti](http://www.tcu.gov.br/fiscalizacaoti)>.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Organização do texto: Juarez de Oliveira. 4. ed. São Paulo: Saraiva, 1990. 168 p.

BRASIL. Gabinete de Segurança Institucional. Portaria n.2. s.l. : Diário Oficial da União, de 8 de fevereiro de 2008.

BRASIL. GSI/PR; (Org) Mandarin Junior, Raphael; Canongia, Cláudia. **Livro Verde: Segurança Cibernética**. 63. Brasília : Brasil, 2010.  
Disponível em: <<http://dsic.planalto.gov.br>>.

BRASIL. Instrução Normativa GSI nº 1, de 13 de junho de 2008. Brasília, 2008b. Disponível em: <<http://dsic.planalto.gov.br/>>. Acesso em: 11 jun. 2012.

BRASIL. Marcela D'alessandro. Dataprev (Org.). **Dataprev fala sobre experiência de Governança de TI durante ENTI**. Disponível em: <<http://portal.dataprev.gov.br/tag/governanca/>>. Acesso em: 27 out. 2011.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. GABINETE DE SEGURANÇA INSTITUCIONAL. (Org) CANONGIA, Cláudia; GONÇALVES JUNIOR, Admilson; MANDARINO JUNIOR, Raphael; **Guia de Referência para a Segurança das Infraestruturas Críticas da Informação**. Brasília: GSIPR/SE/DSIC, 2010. p. 151.

BRITO, Antonio Carlos Pereira de. **Estudo do Gerenciamento de Projeto Baseado no PMBOK para a Implantação da Gestão de Segurança da Informação e Comunicação na Administração Pública Federal**. Brasília: UNB MONOGRAFIA, 2009.

CARUSO, Carlos A. A. e STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. 2ª Edição Revista e Ampliada. São Paulo: Senac, 1999.

CARVALHO, Paulo Sérgio de Melo. **Conferência de Abertura: O setor cibernético nas Forças Armadas Brasileiras**. Brasília: s.n., 2011. pp. 13 - 34. Revista Desafios Estratégicos para Segurança e Defesa Cibernética.

COSTA, Rosa. **Agora, é o presidente do TCU que acusa a Dataprev de corrupção**. O Estado de São Paulo, São Paulo, 21 jan. 2005, p. A5-A5. Disponível em: <<http://www2.senado.gov.br/bdsf/item/id/69610>>. Acesso em: 25 maio 2012.

CRONKHITE, Cathy e MCCULLOUGH, Jack. **Hackers Acesso Negado: Guia completo para proteção dos seus negócios On-line**. Rio de Janeiro: Campus, 2001.

DSIC. 2012. **DSIC**. [Online] 2012. [Citado em: 30 de 08 de 2012.] Disponível em: <<http://dsic.planalto.gov.br/organograma>>.

—. 2010. **GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO**. Brasília: s.n., 2010. Vol. 1, Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior (Org.).

DSIC, Departamento de Segurança da Informação e Comunicações. [Online] 29 de dezembro de 2010. [De acordo com o Artigo 6º do Decreto Nº 7.411, de 29 de dezembro de 2010. Disponível em: <<http://dsic.planalto.gov.br/missao>>. Acesso em: 20 de setembro de 2012.

FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário Eletrônico Aurélio**. 7.0 Curitiba: Positivo, 2010. CD-ROM.

GROUP., Miniwatts Marketing (Org.). **Internet World Stats: usage and Population Statistics**. Disponível em: <<http://www.internetworldstats.com/stats.htm>>. Acesso em: 29 jul. 2012.

IT GOVERNANCE INSTITUTE (Org.). **INFORMATION SECURITY GOVERNANCE: GUIDANCE FOR BOARDS OF DIRECTORS AND EXECUTIVE MANAGEMENT**. 2. ed. United State Of America: Isaca, 2006. Disponível em: <[www.itgi.org](http://www.itgi.org)>. Acesso em: 27 maio 2012.

FERNANDES, Aguinaldo Aragon; Abreu, Vladimir Ferraz de. **Implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços**. Rio de Janeiro: BRASPORT, 2012.

FERRARI, Bruno, CORNACHINE, Daniella; LOYOLA, Leandro. **A Guerra Virtual Começou**. São Paulo: Abril, 2011. pp. 92 - 104. 27 jun 2011.

FONTES, Edson. **Segurança da Informação: O usuário faz a diferença**. São Paulo: Saraiva, 2006. p. 172.

GROSSMANN, Luís Osvaldo. **Convergência Digital**. *www.convergenciadigital.uol.com.br*. [Online] 09 de Setembro de 2009. [Citado em: 12 de Setembro de 2012.] <<http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=20226&sid=11>>.

INFOSEC COUNCIL. 2005. **Computerworld**. [Online] 2005. [Citado em: 20 de SETEMBRO de 2012.] <<http://computerworld.uol.com.br/gestao/2006/08/11/idgnoticia.2006-08-11.6447350724/>>.

ISACA. 2007. **COBIT**. [Online] 2007. [Citado em: 19 de setembro de 2012.] <<http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx>>.

ITGI. 2006. **Information Security Governance**. [Online] 2006. [Citado em: 2012 de Maio de 19.] <<http://www.itgi.org/>>.

ITI. [Online] [Citado em: 31 de 08 de 2012.] <<http://www.iti.gov.br/twiki/bin/view/ITI/Apresentacao>>.

LIBICKI, Martin C. **What Is Information Warfare?** [Online] maio de 1995. [Citado em: 29 de outubro de 2012.] <[http://www.dodccrp.org/files/Libicki\\_What\\_Is.pdf](http://www.dodccrp.org/files/Libicki_What_Is.pdf)>.

MAGALHÃES, Ivan Luizio e PINHEIRO, Walfrido Brito. **Gerenciamento de Serviços de TI, Uma abordagem com base na ITIL**. São Paulo: Novatec, 2007.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL**. São Paulo: Novatec, 2007.

TRIBUNAL DE CONTAS DA UNIÃO. **Levantamento acerca da governança de tecnologia da informação na Administração Pública Federal**. Brasília: Tcu, 2008.

MANDARINO JUNIOR, Raphael. *Dsiceventos.planalto.gov.br*. [Online] 03 de setembro de 2010. [Citado em: 20 de agosto de 2012.] XXVIII Seminário de Segurança da Informação e Comunicações - Rio de Janeiro/RJ.

Disponível em: <<https://dsiceventos.planalto.gov.br/app/eventos/anon/EventoArqsAnonRel.php?idnEntidade=199>>.

—. 2010. **Segurança e Defesa do Espaço Cibernético Brasileiro**. Recife: CUBZAC, 2010. p. 182.

—. 2009. **Um Estudo Sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro**. Brasília: UNB, 2009. p. 156. Monografia (Especialista) - Curso de Ciência da Computação.

MASIERO, Paulo César. **Ética em Computação**. São Paulo: USP, 2008.

MITNICK, Kevin D. **A arte de Invadir**. São Paulo: Pearson Prentice Hall, 2005.

MONTEIRO, Iná Lúcia Cipriano de Oliveira. **Proposta de um guia para elaboração de políticas de segurança da informação e comunicações em órgãos da administração pública federal**. Brasília: UNB - Departamento de Ciência da Computação, 2009. Monografia de Especialização para Especialista em Gestão de Segurança da Informação e Comunicações.

NBR ISO/IEC 27002. **Tecnologia da Informação**: Código de Prática para Gestão da Segurança da Informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

OLIVEIRA, João Roberto de. **Sistema de Segurança e Defesa Cibernética Nacional**. Desafios Estratégicos. 2011, p. 216.

OLIVEIRA, Marlene de et al (Org). **Ciência da Informação e Biblioteconomia**: Novos Conteúdos e Espaços de atuação. Belo Horizonte: UFMG, 2005. p. 143.

PACHECO, André Luiz Furtado. **Governança de TI**: O Desafio Atual da Administração Pública. [Apresentação .pdf]. Porto de Galinhas, Brasil: s.n., p. 50. Disponível em: <[http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia\\_informacao/documentos\\_tema](http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/documentos_tema)>. Acesso em 05 de Setembro de 2011.

RIBEIRO, Sérgio Luis. **Estratégia de Proteção da Infraestrutura Crítica da Informação e Defesa Cibernética Nacional**. Brasília: s.n., 2011. pp. 145 - 163. Revista: Desafios Estratégicos para Segurança e Defesa Cibernética.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: Uma visão Executiva. Rio de Janeiro: Campus, 2003. p. 156.

SERPRO. Serviço Federal de Processamento de Dados - SERPRO. [www.serpro.gov.br/](http://www.serpro.gov.br/). [Online] 2012. [Citado em: 15 de julho de 2012.] Disponível em: <<https://www.serpro.gov.br/conteudo-oserpro/a-empresa-1>>.

SORJ, Bernardo. **Brasil@povo.com**: A luta contra a desigualdade na Sociedade da Informação. Rio de Janeiro: UNESCO, 2003.

STERBAUER, Reinhold, RUCKENBAUER, Hans; KOLB, Anton. **Cibernética**: Responsabilidade em um mundo interligado pela rede digital. São Paulo: Loyola, 2001.

TCU. 2008. **Boas práticas em Segurança da Informação**. Brasília: Tribunal de Contas da União, 2008.

—. 2012. SEFTI. **história**. [Online] 2012. [Citado em: 31 de 08 de 2012.] [http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia\\_informacao/sobre\\_sefti/historia](http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/sobre_sefti/historia).

VIEIRA, Marconi Fábio. **Gerenciamento de Projetos de Tecnologia da Informação**. 2ª Ed. Rio de Janeiro: Elsevier, 2007. p. 484.

Weill, Peter e Ross, Jeanne W. **Governança de TI**: Tecnologia da Informação. São Paulo: M. Books, 2004. p. 276.



## ANEXO A – QUADRO DOS DISPOSITIVOS LEGAIS DE CARÁTER FEDERAL, RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

Dispositivo	Mandamento Legal	Aspecto da SI
<a href="#">Constituição Federal, art. 5º, inciso X.</a>	Direito à privacidade.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
<a href="#">Constituição Federal, art. 5º, inciso XII.</a>	Direito à privacidade das comunicações.	Sigilo dos dados telemáticos e das comunicações privadas.
<a href="#">Constituição Federal, art. 5º, inciso XIV.</a>	Resguardo do sigilo profissional em caso de ofício que exige a ampla confiança no interesse de quem confia como advogados, padres, médicos, psicólogos, etc.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
<a href="#">Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II.</a>	Direito à informação e ao acesso aos registros públicos.	Disponibilidade das informações constantes nos órgãos públicos.
<a href="#">Constituição Federal, art. 5º, inciso XXXIV.</a>	Direito de petição e de obtenção de certidões em repartições públicas.	Disponibilidade das informações constantes nos órgãos públicos.
<a href="#">Constituição Federal, art. 23, incisos III e IV.</a>	Dever do Estado de proteger os documentos e obras.	Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
<a href="#">Constituição Federal, art. 216, § 2º.</a>	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.
<a href="#">Constituição Federal, art. 37, caput.</a>	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.
<a href="#">Constituição Federal, art. 37, § 6º.</a> <a href="#">Código Civil, arts. 927 e 932caput, III.</a>	Responsabilidade objetiva do Estado e das pessoas de direito privado prestadoras de serviços públicos pelos danos causados a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.	Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.
<a href="#">Constituição Federal, art. 37, § 7º.</a>	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.
<a href="#">Consolidação das Leis do Trabalho - CLT, art. 482, alínea g.</a>	Rescisão de contrato de trabalho de empregado que viola segredo da empresa.	Proteção das informações sigilosas acessadas no exercício de emprego público (empresas

Dispositivo	Mandamento Legal	Aspecto da SI
		públicas e sociedades de economia mista).
<a href="#">Código de Conduta da Alta Administração, art. 5º, § 4º.</a>	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)..
<a href="#">Código de Conduta da Alta Administração, art.14, inciso II.</a>	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.
<a href="#">Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea “h” do inciso XV da Seção II.</a>	Proibição de alteração de documentos que devam ser encaminhados para providências.	Proteção da integridade das informações públicas.
<a href="#">Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea “i” do inciso XV da Seção II.</a>	Proibição de retirar da repartição documento ou qualquer outro bem.	Proteção da disponibilidade das informações públicas.
<a href="#">Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso X da Seção I.</a>	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 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.	Proteção da disponibilidade das informações públicas.
<a href="#">Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso VII da Seção I.</a>	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.
<a href="#">Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso IX da Seção I.</a>	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.
<a href="#">Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea “e” do inciso XIV da Seção II.</a>	Dever de aperfeiçoar o processo de comunicação com os usuários para bem servi-los.	Disponibilidade das comunicações.
<a href="#">Código de Defesa do Consumidor, arts. 43 e 44.</a>	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.

Dispositivo	Mandamento Legal	Aspecto da SI
<a href="#">Código Penal, art. 151.</a>	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.
<a href="#">Código Penal, art. 152.</a>	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.
<a href="#">Código Penal, art. 153, § 1º-A.</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.
<a href="#">Código Penal, art. 154.</a>	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.
<a href="#">Código Penal, art. 184, § 3º.</a>	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.
<a href="#">Código Penal, art. 297.</a>	Pena de 2 a 6, e multa por crime de falsificação de documento público.	Proteção da integridade e autenticidade dos documentos públicos.
<a href="#">Código Penal, art. 298.</a>	Pena de 1 a 6 anos, e multa por crime de falsificação de documento particular.	Proteção da integridade e autenticidade dos documentos particulares.
<a href="#">Código Penal, art. 305.</a>	Pena de 2 a 6 anos e multa por crime de supressão, destruição ou ocultação de documento público ou particular.	Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
<a href="#">Código Penal, art. 307.</a>	Pena de 3 meses a 1 ano, ou multa por crime de falsa identidade.	Proteção da autenticidade.
<a href="#">Código Penal, art. 311-A.</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.
<a href="#">Código Penal, art. 313-A.</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 Pública, alteração ou exclusão de dados corretos.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
<a href="#">Código Penal, art. 313-B.</a>	Pena de 3 meses a 2 anos e	Proteção da integridade e

Dispositivo	Mandamento Legal	Aspecto da SI
	multa por crime de modificação ou alteração não autorizada de sistemas de informações.	disponibilidade das informações constantes nos órgãos e entidades públicos.
<a href="#">Código Penal, art. 314.</a>	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.
<a href="#">Código Penal, art. 325.</a>	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.
<a href="#">Código Processo Penal, art. 20.</a>	Sigilo do inquérito policial	Proteção de informações sigilosas.
<a href="#">Código Processo Penal, art. 207.</a>	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.
<a href="#">Código Processo Penal, art. 745.</a>	Sigilo do processo de reabilitação do condenado.	Proteção de informações sigilosas relacionadas ao condenado.
<a href="#">Código Tributário Nacional, art. 198.</a>	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.
<a href="#">Código de Processo Civil, art. 347, inciso II c/c art.363, inciso IV.</a>	Direito da parte de guardar sigilo profissional.	Proteção da privacidade de seus clientes.
<a href="#">Código de Processo Civil, art. 406, inciso II c/c art. 414, § 2º.</a>	Direito da testemunha de guardar sigilo profissional.	Proteção da privacidade de seus clientes.
<a href="#">Lei nº 6.538/78, art. 5º.</a>	Direito a inviolabilidade dos serviços postais e de telegramas.	Sigilo da correspondência.
<a href="#">Lei nº 6.538/78, art. 41.</a>	Pena de detenção de 3 meses a 1 ano, ou multa por violação de sigilo profissional por funcionário do serviço postal.	Proteção da privacidade de correspondência.
<a href="#">Lei nº 7.170/83, art. 13.</a>	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
<a href="#">Lei nº 7.232/84, art. 2º, inciso VIII.</a>	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.
<a href="#">Lei nº 7.492/86, art. 18.</a>	Pena de reclusão de 1 a 4 anos e	Proteção das informações

Dispositivo	Mandamento Legal	Aspecto da SI
	multa por crime de violação de sigilo bancário.	sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.
<a href="#">Lei nº 8.027/90, artigo 2º, inciso V, alínea “a” e inciso VII.</a>	Deveres do Funcionário Público Civil.	Proteção as informações protegidas pelo sigilo.
<a href="#">Lei nº 8.027/90, artigo 5º, inciso I.</a>	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.
<a href="#">Lei nº 8.027/90, art. 5º, parágrafo único, inciso V.</a>	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.
<a href="#">Lei nº 8.112/90, art. 116, inciso VIII.</a>	Dever do servidor de guardar sigilo sobre assunto da repartição.	Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.
<a href="#">Lei nº 8.112/90, art. 132, inciso IX.</a>	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.
<a href="#">Lei nº 8.137/90, art. 3º, inciso I.</a>	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 função; sonegá-lo, ou inutilizá-lo, total ou parcialmente, acarretando pagamento indevido ou inexato de tributo ou contribuição social.	Proteção da disponibilidade de informações para manutenção da ordem tributária.
<a href="#">Lei nº 8.429/92, art.11, incisos III, IV e VII.</a>	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.
<a href="#">Lei nº 8.429/92, art. 13.</a>	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.

Dispositivo	Mandamento Legal	Aspecto da SI
<a href="#">Lei nº 8.443/92, art. 86, inciso IV.</a>	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.
<a href="#">Lei Complementar nº 75/93, art. 8º incisos II, VIII e §§ 1º e 2º.</a>	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.
<a href="#">Lei nº 8.625/93, art. 26, inciso I, alínea "b" e inciso II.</a>	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.
<a href="#">Lei nº 8.906/94, art. 7º, inciso XIX.</a>	Direito do advogado de resguardar o sigilo profissional.	Proteção da privacidade do cliente do advogado.
<a href="#">Lei nº 9.100/95, art. 67, incisos VII e VIII.</a>	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	Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.



Dispositivo	Mandamento Legal	Aspecto da SI
	utilizado pelo serviço eleitoral (Reclusão de 3 a 6 anos).	
<a href="#">Lei nº 9.279/96, art. 75.</a>	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.
<a href="#">Lei nº 9.279/96, art. 195, inciso XI.</a>	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 sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato.	Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.
<a href="#">Lei nº 9.296/96, art. 10.</a>	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.
<a href="#">Lei nº 9.472/97, art. 3º, inciso V.</a>	O usuário de serviços de telecomunicações tem direito à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucionais e legalmente previstas.	Sigilo das comunicações.
<a href="#">Lei nº 9.472/97, art. 3º, inciso VI.</a>	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.
<a href="#">Lei nº 9.472/97, art. 3º, inciso IX.</a>	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.
<a href="#">Lei nº 9.504/97, art. 72.</a>	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	Proteção da integridade das informações de caráter eleitoral e dos equipamentos.

Dispositivo	Mandamento Legal	Aspecto da SI
	usados pelo serviço eleitoral; causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.	
<a href="#">Lei nº 9.605/98, art. 62.</a>	Pena de 1 a 3 anos e multa pela conduta de destruir, inutilizar ou deteriorar arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar protegido por lei, ato administrativo ou decisão judicial.	Disponibilidade e integridade de dados e informações.
<a href="#">Lei nº 10.683/03, art. 6º, inciso IV.</a>	Prevê a competência do GSIPR de coordenar a atividade de segurança da informação.	Todos os aspectos da segurança da informação.
<a href="#">Lei n.º 10.703/03, arts. 1º, 2º e 3º, de 18 de julho de 2003.</a>	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.
<a href="#">Decreto nº 3.505/00, art. 1º.</a>	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.	Pressupostos básicos da segurança da informação.
<a href="#">Decreto nº 4.801/03, art. 1º, inciso X.</a>	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.
<a href="#">Decreto nº 5.483/05, arts. 3º e 11.</a>	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.
<a href="#">Decreto nº 5.687/06, arts. 10 e 13 do Anexo.</a>	Convenção das Nações Unidas contra a Corrupção aprovada pelo Congresso Nacional e promulgada pelo Decreto nº 5.687/06, segundo a qual, cada	Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.



Dispositivo	Mandamento Legal	Aspecto da SI
	<p>Estado signatário deve esforçar-se para implementar, entre outras, as seguintes medidas:</p> <p>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;</p> <p>- 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.</p>	
<p><a href="#">Decreto nº 6.029/07, art 1º, inciso II.</a></p>	<p>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.</p>	<p>Disponibilidade das informações constantes nos registros públicos</p>
<p><a href="#">Decreto nº 6.029/07, art. 10.</a></p>	<p>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.</p>	<p>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.</p>
<p><a href="#">Decreto nº 6.029/07, art. 13.</a></p>	<p>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”.</p>	<p>Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.</p>
<p><a href="#">Decreto nº 6.029/07, art. 22.</a></p>	<p>Comissão de Ética Pública manterá banco de dados de sanções aplicadas para fins de consulta antes de novas</p>	<p>Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética</p>

Dispositivo	Mandamento Legal	Aspecto da SI
	nomeações.	Pública.

**Tabela 10 - Dispositivos Legais Federais de segurança da Informação  
(<http://dsic.planalto.gov.br>, 2012)**

## ANEXO B - QUADRO DA LEGISLAÇÃO ESPECÍFICA DE CARÁTER FEDERAL RELACIONADA À SEGURANÇA DA INFORMAÇÃO

Regulamento	Assunto
<a href="#">Lei nº 7.232, de 29 de outubro de 1984.</a>	Dispõe sobre a Política Nacional de Informática, e dá outras providências.
<a href="#">Lei nº 8.248, de 23 de outubro de 1991.</a>	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
<a href="#">Lei nº 9.296, de 24 de julho de 1996.</a>	Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.
<a href="#">Lei nº 9.472, de 16 de julho de 1997.</a>	Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.
<a href="#">Lei nº 9.507, de 12 de novembro de 1997.</a>	Regula o direito de acesso a informações e disciplina o rito processual do <i>habeas data</i> .
<a href="#">Lei nº 9.609, de 19 de fevereiro de 1998.</a>	Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
<a href="#">Lei nº 9800, de 26 de maio de 1999.</a>	Permite às partes a utilização de sistema de transmissão de dados para a prática de atos processuais.
<a href="#">Lei nº 9.883, de 07 de dezembro de 1999.</a>	Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.
<a href="#">Lei nº 8.159/91, de 08 de janeiro de 2001.</a>	Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.
<a href="#">Lei Complementar nº 105, de 10 de janeiro de 2001.</a>	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
<a href="#">Medida Provisória nº 2.200-2, de 24 de agosto de 2001.</a>	Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.
<a href="#">Lei nº 10.973, de 02 de dezembro de 2004.</a>	Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.
<a href="#">Lei nº 11.419, de 19 de dezembro de 2006.</a>	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.
<a href="#">Lei nº 12.527 de 18 de</a>	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

<a href="#">novembro de 2011 (LAI).</a>	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.
<a href="#">Decreto nº 2.295, 04 de agosto de 1997.</a>	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.
<a href="#">Decreto nº 2.556, de 20 de abril de 1998.</a>	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.
<a href="#">Decreto nº 3.294, de 15 de dezembro de 1999.</a>	Institui Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.
<a href="#">Decreto nº 3.505, de 13 de junho de 2000.</a>	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
<a href="#">Decreto de 18 de outubro de 2000.</a>	Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.
<a href="#">Decreto nº 3.714, 03 de janeiro de 2001.</a>	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.
<a href="#">Decreto nº 3.996, de 31 de outubro de 2001.</a>	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
<a href="#">Decreto nº 4.073, de 03 de janeiro de 2002.</a>	Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.
<a href="#">Decreto nº 4.376, de 13 de setembro de 2002.</a>	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.
<a href="#">Decreto nº 4.414, de 07 de outubro de 2002.</a>	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.
<a href="#">Decreto nº 4.522, de 17 de dezembro de 2002.</a>	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.
<a href="#">Decreto nº 4.553, de 27 de dezembro de 2002.</a>	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
<a href="#">Decreto nº 4.689, de 07 de maio de 2003.</a>	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da

	Informação – ITI, e dá outras providências.
<a href="#"><u>Decreto nº 4.829, de 03 de setembro de 2003.</u></a>	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.
<a href="#"><u>Decreto de 29 de outubro de 2003.</u></a>	Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências.
<a href="#"><u>Decreto nº 5.301, de 09 de dezembro de 2004.</u></a>	Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.
<a href="#"><u>Decreto nº 5.450, de 31 de maio de 2005.</u></a>	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
<a href="#"><u>Decreto nº 5.563, de 11 de outubro de 2005.</u></a>	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.
<a href="#"><u>Decreto nº 5.584, de 18 de novembro de 2005.</u></a>	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.
<a href="#"><u>Decreto nº 6.605, de 14 de outubro de 2008.</u></a>	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.
<a href="#"><u>Decreto nº 7.724 de 16 de maio de 2012.</u></a>	Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do <b>caput</b> do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.
<a href="#"><u>Instrução Normativa nº 1 do GSI, de 13 de junho de 2008.</u></a>	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
<a href="#"><u>Resolução nº 58 do INPI, de 14 de julho de 1998.</u></a>	Estabelece normas e procedimentos relativos ao registro de programas de computador.
<a href="#"><u>Resolução nº 59 do INPI, de 14 de julho de 1998.</u></a>	Estabelece os valores das retribuições pelos serviços de registro de programas de computador.
<a href="#"><u>Resolução nº 132 do STM, de 02 de fevereiro de 2005.</u></a>	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.
<a href="#"><u>Resolução nº 338 do STF, de 11 de abril de 2007.</u></a>	Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do Superior Tribunal de Federal - STF.

<a href="#"><u>Resolução nº 140 do TST, de 13 de setembro de 2007.</u></a>	Regulamenta, no âmbito da Justiça do Trabalho, a Lei nº 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.
<a href="#"><u>Resolução nº 23.370/11 do TSE, de 13 de dezembro de 2011.</u></a>	Dispõe sobre a propaganda eleitoral e as condutas ilícitas em campanha eleitoral nas eleições de 2012. (Propaganda Eleitoral na Internet - art. 18 a 25).

**Tabela 11 - Legislação Específica Federal de Segurança da Informação (<http://dsic.planalto.gov.br>, 2012)**

## ANEXO C - ALGUNS PROJETOS DE LEI RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

Regulamento	Assunto e autoria
<a href="#">Projeto de Lei nº 84/1999.</a>	Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Autor: Deputado Luiz Piauhyllino.
<a href="#">Projeto de Lei nº 3.494/2000.</a>	Altera a lei do “ <i>habeas data</i> ” (Lei nº 9.507, de 12 de novembro de 1997). Autor: Senado Federal.
<a href="#">Projeto de Lei nº 7.316/2002.</a>	Regulamenta o uso de assinaturas eletrônicas e a prestação de serviços de certificação. Autor: Poder Executivo.
<a href="#">Projeto de Lei nº 21/2004.</a>	Proíbe envio de mensagens não solicitadas (spam); estabelece multa; estabelece como nova modalidade do crime de falsidade ideológica a conduta de impedir a identificação do remetente ou o bloqueio automático de mensagens eletrônicas não solicitadas, inserir declaração falsa ou diversa da que deveria constar, com o fim de impossibilitar a identificação da origem ou o rastreamento da mensagem. Autor: Senador Duciomar Costa.
<a href="#">Projeto de Lei nº 1.704/2007.</a>	Tipifica a conduta de violação de comunicação eletrônica. Autor: Deputado Rodovalho.
<a href="#">Projeto de Lei nº 398/2007.</a>	Prevê o aumento de pena no caso de crime contra a honra praticado pela Internet. Autor: Senador Expedito Júnior.
<a href="#">Projeto de Lei nº 1.230/2007.</a>	Torna obrigatória a identificação biométrica para acesso a bancos de dados da administração pública direta, indireta e fundacional onde sejam armazenados dados sensíveis. Autor: Deputado Eduardo Gomes.
<a href="#">Projeto de Lei nº 2.899/2008.</a>	Obriga as operadoras de telefonia fixa e móvel ao pagamento de multa em razão de danos decorrentes da ineficiência em garantir a privacidade de seus usuários. Autor: Deputado William Woo.
<a href="#">Projeto de Lei nº 3.272/2008.</a>	Normatiza a quebra de sigilo das comunicações telefônicas para fins de investigação criminal e instrução processual penal. Revoga a Lei nº 9.296, de 1996; altera o Decreto-Lei nº 2.848, de 1940 e o Decreto-Lei nº 3.689, de 1941. Regulamenta a Constituição Federal de 1988. Autor: Poder Executivo.
<a href="#">Projeto de Lei nº 4.036/2008.</a>	Altera as Leis nº 4.878, de 3 de dezembro de 1965, 8.112, de 11 de dezembro de 1990, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para dispor sobre sanções administrativas e penais aplicáveis em casos de interceptação de comunicações e de violação de sigilo, e dá outras providências. Aumenta a pena para conduta abusiva de interceptação ilegal, “grampo telefônico”. Autor:

Regulamento	Assunto e autoria
	Poder Executivo.
<a href="#">Projeto de Lei nº 3.773/2008.</a>	Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na Internet. Autor: Senado Federal - Comissão Parlamentar de Inquérito – Pedofilia.
<a href="#">Projeto de Lei nº 2126/2011.</a>	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Autor: Poder Executivo.
<a href="#">Projeto de Lei nº 2793/2011.</a>	Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Autor: Deputado Paulo Teixeira.

**Tabela 12 - Projetos de Lei de Segurança da Informação (<http://dsic.planalto.gov.br>, 2012).**



## ANEXO D – TABELA RELACIONAMENTO ISO 17799, COBIT E ITIL

	Objetivos de Controle do COBIT	Objetivos de Controle do COBIT referenciados na ISO 17799	Objetivos de Controle do COBIT referenciados no modelo ITIL
Nível Estratégico	<b>PO - Planejamento e Organização</b>		
	PO1-Definir um Plano Estratégico de TI		
	PO2-Definir a Arquitetura da Informação	X	
	PO3-Determinar a Direção Tecnológica	X	Superficialmente
	PO4-Definir a Organização e Relacionamentos de TI	X	Superficialmente
	PO5-Gerenciar o Investimento em TI		Superficialmente
	PO6-Comunicar metas e diretivas gerenciais	X	
	PO7-Gerenciar Recursos Humanos	X	
	PO8-Garantir Conformidade com Requisitos Externos	X	
	PO9-Avaliar Riscos	X	
	PO10-Gerenciar Projetos		
	PO11-Gerenciar Qualidade		
Nível Operacional e Nível Tático	<b>AI - Aquisição e Implementação</b>		
	AI1-Identificar Soluções Automatizadas	X	X
	AI2-Adquirir e Manter Software Aplicativo	X	X
	AI3-Adquirir e Manter Infra-estrutura Tecnológica	X	X
	AI4-Desenvolver e Manter Procedimentos	X	X
	AI5-Instalar e Validar Sistemas	X	X
	AI6-Gerenciar Mudanças	X	X
	<b>DS - Entrega e Suporte</b>		
	DS1-Definir e Gerenciar Níveis de Serviço	X	X
	DS2-Gerenciar Serviços de Terceiros	X	X
	DS3-Gerenciar Desempenho e Capacidade	X	X
	DS4-Garantir Continuidade dos Serviços	X	X
	DS5-Garantir Segurança de Sistemas	X	
	DS6-Identificar e Alocar Custos		X
	DS7-Educar e Treinar Usuários	X	
	DS8-Auxiliar e Aconselhar Clientes	X	X
	DS9-Gerenciar Configuração	X	X
	DS10-Gerenciar Problemas e Incidentes	X	X
	DS11-Gerenciar Dados	X	X
	DS12-Gerenciar instalações	X	
DS13-Gerenciar a Operação	X	X	
Nível Estratégico	<b>M - Monitoramento</b>		
	M1-Monitorar os Processos	X	
	M2-Avaliar a Adequação do Controle Interno	X	
	M3-Obter certificação Independente		
	M4-Providenciar Auditoria Independente		

**Tabela 13 - Relacionamento de Processos entre os modelos ITIL e COBIT e a norma ISO 17799 (BERNARDES, et al., 2005).**

## ANEXO E – FATOS RECENTES

Costa (2005) cita no Jornal O Estado de São Paulo um caso onde a falta de gestão efetiva na DATAPREV para informações críticas. Para evitar a má fé seria exigível houvesse forma de controle que previsse a possibilidade de acesso a ambientes não autorizados (FONTES ,2006, p.40).

Uma semana depois de o ministro da Previdência Social, Amir Lando, ter declarado ao Estado que há grupos no governo "empenhados em derrubá-lo do cargo por causa de sua batalha contra as fraudes na Dataprev", o presidente do Tribunal de Contas da União (TCU), ministro Adylson Motta, apontou a **base de dados da empresa como um dos principais focos de corrupção no País** [grifo meu]. Segundo ele, houve mesmo o caso de um técnico do tribunal que, diante de testemunhas, acessou o sistema com a senha comum de usuário, entrou na listagem de uma aposentadoria comum, de seu pai, alterou o valor e saiu de lá sem ser incomodado. "E tudo isso foi testemunhado", destacou. "Veja a fragilidade do sistema, se ele alterou uma aposentadoria, pode alterar todas porque o sistema é falho." O desabafo de Lando custou-lhe uma cobrança do presidente Luiz Inácio Lula da Silva, em reunião no Palácio do Planalto, e provavelmente o cargo na reforma ministerial, quando poderá ser substituído pelo senador Romero Jucá (PMDB-RR) ou pelo senador Maguito Vilella (PMDB-GO). A Dataprev, por sua vez, divulgou uma nota repudiando a acusação do ministro da Previdência. Na quarta-feira, a Associação Nacional dos Empregados das Empresas de Tecnologia e Informações da Previdência Social também considerou "absurda" a acusação feita por Lando. Agora, a associação está tentando entregar ao ministro da Casa Civil, José Dirceu, um abaixo-assinado cobrando investimentos na Dataprev. O presidente do TCU disse que comunicou o episódio da troca de valor da aposentadoria a dois ex-ministros da Previdência, Waldeck Ornelas e Roberto Brant. "Os dois mostraram preocupação ali, na hora, mas a coisa continua", afirmou. "Tem de ser uma fiscalização permanente lá dentro." [...]. "Na Previdência, mesmo que não tenhamos parceria, vamos fazer um acompanhamento permanente." Motta previu que o ministro será receptivo à medida. "Tenho certeza de que o ministro Amir Lando acolherá a iniciativa com o maior entusiasmo porque ele está preocupadíssimo com as fraudes da Previdência." Ele insistiu na necessidade de "pôr lá dentro uma equipe do TCU, fazer um acompanhamento permanente com a colaboração de técnicos de lá, do controle externo, da Procuradoria".

A rede do serviço federal de processamento de dados (Serpro) foi noticiada no site da Idgnow (2005, apud, FONTES, 2006, p.69) conforme abaixo:

A rede do Serviço Federal de Processamento de Dados (SERPRO), prestador de serviços em tecnologia da informação vinculado ao Ministério da Fazenda, foi atacada por variantes da praga virtual Agobot (AFQ) desde sexta-feira (21/01). Conforme explica Sérgio Rosa, diretor do Serpro, o ataque foi caracterizado por uma sobrecarga de mensagens eletrônicas ao servidor web do órgão, mas não afetou os bancos de dados da instituição. "A sobrecarga fez com que o acesso a e-mails e sites de serviços do Serpro ficassem lentos e até paralisados", informou Rosa. Segundo a assessoria de comunicação do Serpro, o primeiro ataque foi identificado no final de

semana pela Trend Micro, uma das fornecedoras de sistemas de segurança do Serpro e uma vacina solucionou o problema na segunda-feira (24/01). Entretanto, nesta quarta-feira (26/01), a rede voltou a ser alvo de outra variante do Agobot, que voltou a causar lentidão no acesso aos serviços do Serpro. Segundo Rosa, a rede está normalizada.

A empresa informa que "todos os sistemas do governo, incluindo os críticos como como Siafi, ReceitaNet e Siscomex, mantém suas bases de dados íntegras, em ambientes isolados e seguros".

Para evitar novos ataques à rede do Serpro, Sergio Rosa destaca uma solução tática e outra estratégia. A tática envolve a atenção e o combate às pragas, sabendo que há o risco de receber uma ameaça ainda não identificada pelos fornecedores de segurança de dados. A estratégica compreende a migração de toda a rede do Serpro para o sistema operacional Linux de código-fonte aberto.

"Hoje trabalhamos com plataforma Microsoft, Novell e a solução livre, mas a migração para Linux evita esse tipo de problema", diz Rosa. Atualmente, 60% das 10 mil estações de trabalho do Serpro rodam em Linux e a expectativa é finalizar a mudança até o final de 2005.

## **ANEXO F – TESTE DE CONFORMIDADE COM A NORMA ISO/IEC 17799 (SÊMOLA, 2003)**

### **Objetivo:**

Permitir a sua percepção quanto ao grau de conformidade que a organização tem em relação aos controles sugeridos pelo código de conduta de gestão de segurança da informação definidos pela norma ISO/IEC 17799.

### **Instruções:**

Escolha apenas uma resposta para cada pergunta e contabilize os pontos ao final.

#### Política de segurança

1. Política de segurança?

A- Sim

B- Sim, porém desatualizada.

C- Não

2. Algum responsável pela gestão da política de segurança?

A- Sim

B- Sim, porém não está desempenhando esta função.

C- Não

#### Segurança organizacional

3. Infraestrutura de segurança da informação para gerenciar as ações corporativas?

A- Sim

B- Sim, porém desatualizada.

C- Não

4. Fórum de segurança formado pelo corpo diretor a fim de gerir mudanças estratégicas?

A- Sim

B- Sim, mas não está sendo utilizado atualmente.

C- Não

5. Definição clara das atribuições de responsabilidade associadas à segurança da informação?

A- Sim

B- Sim, porém desatualizada.

C- Não

6. Identificação dos riscos no acesso de prestadores de serviço?

A- Sim

B- Sim, porém desatualizada.

C- Não

7. Controle de acesso específico para os prestadores de serviço?

A- Sim

B- Sim, porém desatualizado.

C- Não

8. Requisitos de segurança dos contratos de terceirização?

A- Sim

B- Sim, porém desatualizados.

C- Não

#### Classificação e controle dos ativos de informação

9. Inventário dos ativos físicos, tecnológicos e humanos?

A- Sim

B- Sim, porém desatualizado.

C- Não

10. Critérios de classificação da informação?

A- Sim

B- Sim, porém desatualizados.

C- Não

#### Segurança em pessoas

11. Critérios de seleção e política de pessoal?

A- Sim

B- Sim, porém desatualizados.

C- Não

12. Acordo de confidencialidade, termos e condições de trabalho?
- A- Sim
  - B- Sim, porém desatualizados.
  - C- Não
13. Processos para capacitação e treinamento de usuários?
- A- Sim
  - B- Sim, porém desatualizados.
  - C- Não
14. Estrutura para notificar e responder aos incidentes e falhas de segurança?
- A- Sim
  - B- Sim, porém desatualizada.
  - C- não

Segurança física e de ambiente

15. Definição de perímetros e controles de acesso físico aos ambientes?
- A- Sim
  - B- Sim, porém desatualizada.
  - C- Não
16. Recursos para segurança e manutenção dos equipamentos?
- A- Sim
  - B- Sim, porém desatualizados.
  - C- Não
17. Estrutura para fornecimento adequado de energia?
- A- Sim
  - B- Sim, porém desatualizada.
  - C- Não
18. Segurança do cabeamento?
- A- Sim
  - B- Sim, porém desatualizada.
  - C- Não

Gerenciamento das operações e comunicações

19. Procedimentos e responsabilidades operacionais?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

20. Controle de mudanças operacionais?

- A- Sim
- B- Sim, porém desatualizado.
- C- Não

21. Segregação de funções e ambientes?

- A- Sim
- B- Sim, porém desatualizada.
- C- Não

22. Planejamento e aceitação de sistemas?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

23. Procedimentos para cópias de segurança?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

24. Controles e gerenciamento de Rede?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

25. Mecanismos de segurança e tratamento de mídias?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

26. Procedimentos para documentação de sistemas?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

27. Mecanismos de segurança do correio eletrônico?

- A- Sim

B- Sim, porém desatualizados.

C- Não

#### Controle de acesso

28. Requisitos do negócio para controle de acesso?

A- Sim

B- Sim, porém desatualizados.

C- Não

29. Gerenciamento de acessos do usuário?

A- Sim

B- Sim, porém desatualizado.

C- Não

30. Controle de acesso à rede?

A- Sim

B- Sim, porém desatualizado.

C- Não

31. Controle de acesso ao sistema operacional?

A- Sim

B- Sim, porém desatualizado.

C- Não

32. Controle de acesso às aplicações?

A- Sim

B- Sim, porém desatualizado.

C- Não

33. Monitoração do uso e acesso ao sistema?

A- Sim

B- Sim, porém desatualizado.

C- Não

34. Critérios para computação móvel e trabalho remoto?

A- Sim

B- Sim, porém desatualizados.

C- Não

#### Desenvolvimento e manutenção de sistemas



35. Requisitos de segurança de sistemas?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

36. Controles de criptografia?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

37. Mecanismos de segurança nos processos de desenvolvimento e suporte?

- A- Sim
- B- Sim, porém desatualizados.
- C- Não

#### Gestão da continuidade do negócio

38. Processo de gestão da continuidade do negócio?

- A- Sim
- B- Sim, porém desatualizado.
- C- Não

#### Conformidade

39. Gestão de conformidades técnicas e legais?

- A- Sim
- B- Sim, porém desatualizado.
- C- Não

40. Recursos e critérios para auditoria de sistemas?

- A- Sim
- B- Sim, porém desatualizado.
- C- Não

#### **Tabela de pontuação**

Some os pontos correspondentes às respostas de acordo com a tabela abaixo:

Resposta A: some 2 pontos
---------------------------

Resposta B: some 1 ponto

Resposta C: não some nem subtraia pontos

### **Índices de Conformidade com a norma ISO 17799**

Veja agora a que distância está da conformidade com a norma.

#### Resultado entre 80-54

Parabéns! Sua empresa é uma exceção e deve estar em destaque em seu segmento de mercado por conta da abrangência dos controles que aplica no negócio. Apesar de não podermos ver a uniformidade das ações, distribuídas pelos 10 domínios, podemos dizer que sua empresa está conscientizada da importância da segurança para a saúde dos negócios. A situação estará ainda melhor se todas as ações e controles aplicados tiverem sido decididos com base em uma análise de riscos integrada e ainda sob a gestão de um Security Officer.

#### Resultado entre 53-27

Atenção! Este resultado pode ter sido alcançado de diversas formas. Sua empresa pode ter adotado quase que a totalidade dos controles, mas a maioria dos quesitos pode estar defasada, desatualizada ou inativa, o que demonstraria um bom nível de consciência, mas também deficiência na estrutura de gestão ou a falta de fôlego financeiro para subsidiar os recursos de administração. Poderia ainda ter parcela representativa dos controles em ordem, deixando os demais inoperantes, ou mesmo inexistentes. Diante disso, é conveniente alertarmos para a grande possibilidade de evolução, bem como a possibilidade de estagnação e de redução tendenciosa do nível de segurança por falta de orientação. Mais uma vez, a ausência de uma análise de riscos pode ser a causa para a desorientação dos investimentos e a dificuldade de priorização das atividades.

### Resultado entre 26-0

Cuidado! A situação não é confortável para a empresa. A segurança da informação não está sendo tratada como prioridade e a pontuação indica a ausência ou ineficácia de muitos dos controles recomendados pela norma. As causas podem ser o desconhecimento dos riscos e a falta de sensibilização dos executivos e da alta administração. Arrisco dizer que seu segmento de mercado não vive um momento muito competitivo ou que a segurança não seja vista por seus clientes como um fator crítico de sucesso por conta da natureza de sua atividade. Outra hipótese é que devem estar ocorrendo ações isoladas - de um departamento ou de outro - que apesar de louváveis, não distribuem uniformemente a segurança e acabam por minimizar o aumento do nível de segurança do negócio. Apesar de tudo, não é hora de desanimar. Sempre há tempo de reverter a situação. Comece com uma análise de riscos e boa sorte.

**ANEXO G – ARTIGO**

# Governança de Segurança da Informação para Defesa Cibernética da Administração Pública Federal

Alexandre Henrique

Departamento de Informática e Estatística (INE)  
Universidade Federal de Santa Catarina (UFSC) - Florianópolis – SC – Brasil

henri.sgt@inf.ufsc.br

**Resumo.** *A Governança de Segurança da Informação aplicada para Defesa Cibernética da Administração Pública Federal proposta neste trabalho se dá por meio dos modelos COBIT, ITIL, norma ISO 17799 e PMBOK. A partir desses modelos, sob a ótica da segurança cibernética, estão agregados conhecimentos que atingem a estrutura de decisão dos sistemas de informações gerenciais atentando-se para a realidade dos órgãos públicos. Identificado o desafio da situação atual do país principalmente por meio de um levantamento realizado pelo Tribunal de Contas da União é apresentado, para cada um dos modelos, bem como da combinação deles, a definição dos objetivos de controle, definição dos processos e implantação da gestão de segurança cibernética.*

**Abstract.** *Governance of Information Security Cyber Defence applied to the Federal Public Administration proposed in this paper is given by the models COBIT, ITIL, ISO 17799 and PMBOK. From these models, from the perspective of cyber security, are aggregated knowledge that reach the decision structure of management information systems paying attention to the reality of public bodies. Identified the challenge of the current situation of the country mainly through a survey conducted by the Court of Audit is presented for each of the models, and the combination of them, the definition of the control objectives, processes definition and implementation of management cyber security.*

## 1. Espaço Cibernético Brasileiro

Os avanços da tecnologia da informação, as chamadas TICs, promovem incontáveis benefícios para a sociedade da informação. Forma-se, então, uma complexa teia de atores, equipamentos e locais; partes integrantes do que é conhecido como espaço cibernético. Na esfera de um país esse espaço cibernético se assemelha ao próprio território que juntamente com o povo e soberania constituem a “nação virtual brasileira”. Nela há características que causam preocupações para o Estado brasileiro, são elas: a) convergência de tecnologias, aumento significativo de sistemas e redes de informação, aumento crescente de acesso à Internet, avanços das tecnologias de informação e comunicação; b) aumento das ameaças e das vulnerabilidades, apontando para a urgência de ações na direção da criação, manutenção e fortalecimento da cultura de segurança; e, c) ambiente em constante, e rápidas mudanças.

A administração pública federal (APF) deve esforçar-se para construir estratégias de segurança e defesa cibernéticas na nação virtual, bem como o faz na sociedade em geral. Os parâmetros primários de Segurança da Informação e Comunicação (SIC) que a APF almeja assegurar, de acordo com a IN GSIPR N° 01/2008<sup>5</sup>, são: disponibilidade, integridade, confidencialidade e autenticidade das informações. Nesse sentido alguns princípios formam a

---

<sup>5</sup> BRASIL. Instrução Normativa de 13 de junho de 2008. Disciplina a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta. Diário oficial da União, n. 115, 18 jun. 2008.

base para se desenvolver as estratégias de segurança da informação de governo a fim de manter e preservar as infraestruturas críticas do país. Tais princípios são estudados por países membros da Organização para Cooperação e o Desenvolvimento Econômico (OCDE)<sup>6</sup>, e são apresentados na **Tabela 14**.

**Tabela 14 - Princípios para estratégias de segurança**

Sensibilização sobre riscos	Seguir normas e boas práticas, implantar controles, e estar em alerta sobre todo tipo de interconectividade e interdependência de sistemas e redes de informação;
Responsabilidade	Entender a importância de avaliar e atualizar sistematicamente as políticas, práticas, medidas e procedimentos de segurança adotados para sistemas e redes de informação;
Resposta	Agir proativamente e em cooperação, prevenindo, detectando e respondendo aos incidentes;
Ética	Respeitar interesses legítimos de todas as partes envolvidas; elaborar e adotar práticas exemplares na condução da segurança de sistemas e redes de informação;
Democracia	Seguir e fortalecer valores fundamentais de uma sociedade democrática na segurança de sistemas e redes de informação
Avaliação de riscos	Minimizar ameaças e vulnerabilidades por meio de ações que sejam amplas o bastante para englobar os fatores críticos internos e externos (tecnologias, físicos, humanos, políticos, serviços de terceiros)
Concepção	Integrar segurança como elemento essencial no processo de planejamento, modelagem, criação e gestão de sistemas e rede de informação, com soluções inovadoras;
Gestão de Segurança	Coordenar e integrar a avaliação de riscos e a capacidade de resposta e resolução de incidentes, bem como a auditoria de sistemas e redes de informação, para criar um sistema coerente de segurança da informação;
Reavaliação	Examinar e reavaliar a segurança de sistemas e redes de informação, e introduzir as necessárias mudanças nas respectivas políticas, estratégias, medidas e procedimentos.

Segundo Mandarino Junior<sup>7</sup> “segurança cibernética é entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas”. Como infraestrutura crítica da informação o governo brasileiro considera a informação que afeta diretamente a consecução e a continuidade da missão do Estado, incidindo diretamente na segurança da sociedade, de acordo com a Portaria nº 34, de agosto de 2009<sup>8</sup>.

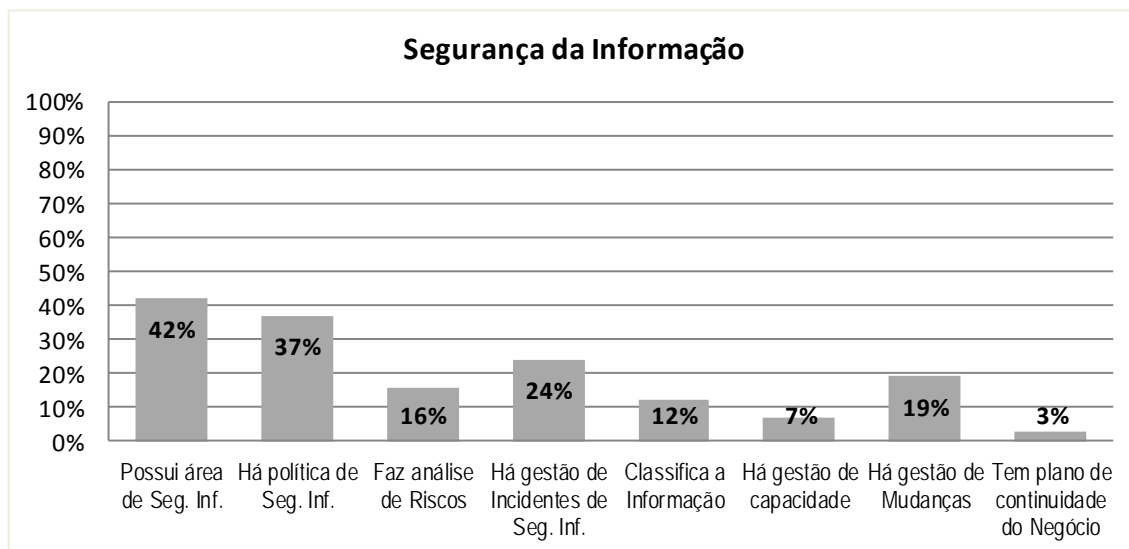
## 2. Segurança da Informação nos Órgãos da APF

<sup>6</sup> Organization for Economic Co-Operation and Development (OECD) - Guidelines for the Security of Information Systems and Networks: Towards a culture of security. (Adopted as a Recommendation of the OECD Council at its 1037 th Session on 25 July 2002). Paris: OECD. 2002. 28p

<sup>7</sup> MANDARINO, R. Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro. 2009. Monografia (especialização). Universidade de Brasília (UnB). Departamento de Ciência da Computação - DCE: Brasília. Jun. 2009. p. 29.

<sup>8</sup> BRASIL. Portaria nº. 34, de 05 de agosto de 2009. Diário Oficial da República Federativa do Brasil, Brasília, 06 ago 2009.

O Tribunal de Contas da União (TCU) realizou um levantamento em 2010<sup>9</sup> com 315 órgãos públicos no qual as informações de segurança da informação se destacaram na Gestão da Governança de Tecnologia da Informação. Os dados relacionados a prática da segurança da informação e comunicações na APF foram mapeados e apresentados conforme o gráfico abaixo:



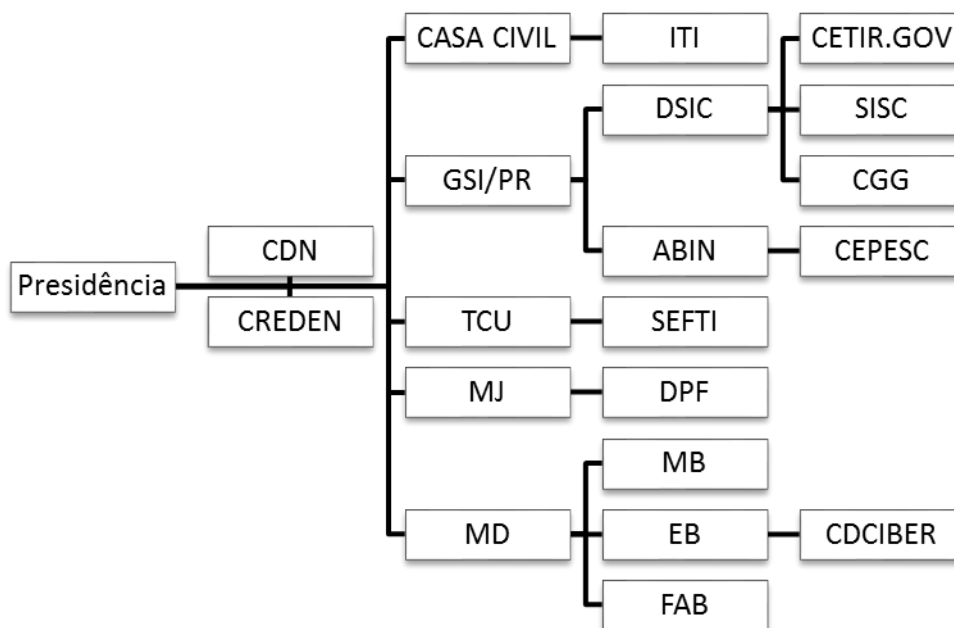
**Gráfico 1 - Indicadores de Segurança da Informação na APF.**

Os conhecimentos obtidos com a pesquisa do TCU, tendo por base as estruturas de tomadas de decisões dos Sistemas de Informações Gerenciais (SIG) da APF, formaram o conjunto de processos passíveis de serem aplicados no planejamento estratégico de segurança da informação. Os controles (o que), processos (como), pessoas (quem) e tecnologia (ferramentas automatizadas), para Governança da Segurança da Informação apresentados neste trabalho são analisados com base em modelos sólidos de governança como COBIT e ISO/IEC 17799 para definições de objetivos de controles; ITIL, para definir os processos; e PMBOK, para implantação da gestão da segurança. Tais práticas devem se encaixar no processo de segurança cibernética da APF e a aplicação alinhada com seu plano estratégico.

No Brasil, importantes agentes do governo participam ativamente na estratégia tanto de segurança da informação quanto de defesa cibernética, uma vez que compreende atitudes de prevenção e repressão, e abrange pessoas e processos. Dessa forma o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por intermédio de seu Departamento de Segurança da Informação e Comunicações (DSIC), trabalha em favor de uma efetiva colaboração entre os representantes de vários órgãos da APF. O GSI/PR colocou em prática a formação do Comitê Gestor de Segurança da Informação (CGSI), a construção de arcabouço normativo, a criação de grupos de trabalhos e técnicos, e a formação de recursos humanos para trabalharem com segurança cibernética. O GSI/PR exerce função de Secretaria-Executiva para o Conselho de Defesa Nacional (CDN) e para a Câmara de Relações Exteriores e Defesa Nacional (CREDEN) agindo também por intermédio deles para tratar de segurança cibernética e assuntos conexos.

Órgãos importantes relacionados ao tema deste trabalho apresentados em uma estrutura hierárquica podem ser identificados na **Figura 31**.

<sup>9</sup> BRASIL, Tribunal de Contas da União (TCU). Levantamento de governança de TI. TCU. Brasília : TCU, 2010. p. 49. Relator Ministro Aroldo Cedraz – Disponível em: <[www.tcu.gov.br/fiscalizacaoti](http://www.tcu.gov.br/fiscalizacaoti)>.



**Figura 31 - Hierarquia dos principais órgãos da APF na segurança e defesa cibernética.**

Devido ao fato de a proteção do Estado ocorrer em várias dimensões, tais quais, população, território e governo; a proteção cibernética em nível nacional envolve setores dedicados à segurança institucional, desse modo a Estratégia Nacional de Defesa (END)<sup>10</sup> atribui papel de destaque para o Ministério da Defesa por meio de suas Forças Armadas. A Marinha do Brasil (MB), o Exército Brasileiro (EB) e a Força Aérea Brasileira (FAB) aplicam seus meios para uso no mais recente campo de combate, o espaço cibernético.



**Figura 32 - Ministério da Defesa - Forças Armadas**

Para cumprir os objetivos característicos da defesa cibernética as atividades das Forças armadas devem abranger: nível estratégico – ações cibernéticas necessárias à atuação das

<sup>10</sup> BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Diário Oficial da União, Poder Executivo, Brasília, DF, 19 dez. 2008.



Forças Armadas em situações de crise ou conflito armado e, até mesmo, em casos esporádicos, em situações de paz ou normalidade institucional, ao receber mandado para isso; nível operacional – ações cibernéticas, defensivas e ofensivas, relativas ao preparo e ao emprego em operações militares, de qualquer natureza e intensidade, que caracterizam um ambiente de guerra cibernética.

O EB tem destaque especial na condução das atividades cibernéticas do MD com o Centro de Defesa Cibernética (CDCiber) e seu Núcleo (NuCiber) que, em linhas gerais, tem como objetivo (OLIVEIRA, 2011)<sup>11</sup>: a) expansão e aprimoramento da estrutura de segurança cibernética já existente; b) expansão e aprimoramento da estrutura de capacitação, adestramento e emprego operacional já existente, para atender, também, às necessidades do Setor Cibernético, incluindo, ainda, os assuntos relacionados ao tema nos currículos dos estabelecimentos de ensino da Força; c) estabelecimento de uma estrutura de apoio tecnológico e de pesquisa cibernética; d) estabelecimento de uma estrutura de gestão de pessoal e de arcabouço documental; e) estabelecimento de uma estrutura para atendimento das necessidades de inteligência voltadas para o setor; f) formatação da estrutura e das missões do Centro de Defesa Cibernética do Exército, a partir do seu Núcleo já ativado.

A árdua tarefa de resguardar a segurança cibernética e assegurar a interação entre os órgãos da APF depende do fluxo das informações em situações de prevenção e de repressão de incidentes de segurança cibernética. Medidas que vão desde capacitação e troca de informações até a preparação para uma situação de guerra cibernética são tomadas de modo coordenado e coerente pelos órgãos envolvidos.

A Tabela 2, a seguir, mostra resumidamente os órgãos em suas características institucionais quanto seu papel na defesa cibernética do país.

**Tabela 15 - Papéis na Segurança e Defesa Cibernética<sup>8</sup>.**

Órgão	Papel			Ação		
	Estratégico	Tático	Operacional	Preventiva	Repressiva	Defensiva
CDN	X			X	X	X
CREDEN	X	X		X	X	X
CASA CIVL	X			X		
ITI		X		X		
GSI	X	X		X		
DSIC		X	X	X		
CTIR		X	X	X	X	
ABIN			X	X		X
MD	X					X
MB	X	X	X			X
EB	X	X	X			X
FAB	X	X	X			X
MJ		X	X	X	X	
PF		X	X	X	X	
TCU	X	X		X		

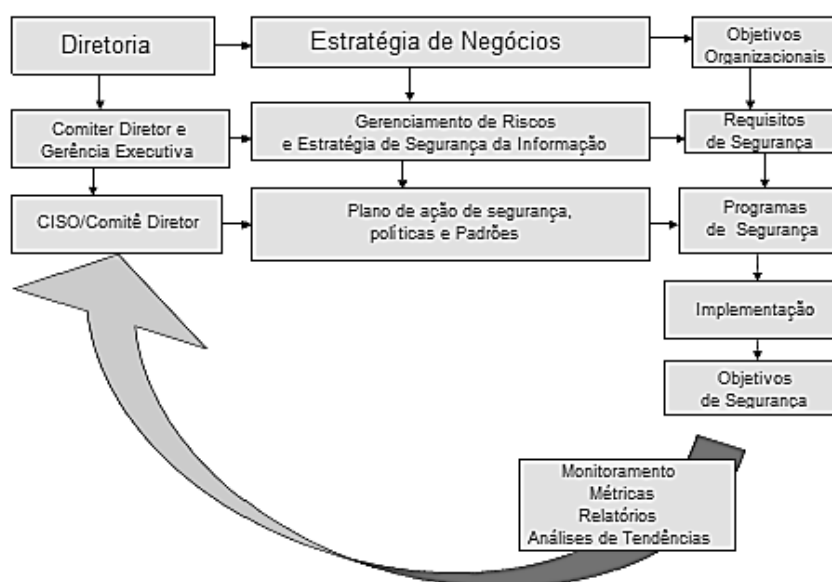
<sup>11</sup> OLIVEIRA, João Roberto de. **Sistema de Segurança e Defesa Cibernética Nacional**. Desafios Estratégicos. 2011, p. 216.

Os aprofundamentos necessários à aplicação dos parâmetros e valores prioritários de SIC recomendados pela Instrução Normativa nº 01/2008, são produzidos e publicados na forma de Normas Complementares (NC), colocadas como ações adicionais e compulsórias para a APF. Tais disciplinas representam desafios a serem implementados em todos os órgãos e entidades da APF, e devem ser construídos de modo aceitável para os requisitos, não permitindo vulnerabilidades diante do cenário atual.

### 3. Propostas de Governança no Cenário Cibernético Brasileiro

A implantação do conjunto de boas práticas em segurança da informação tem por objetivo garantir a disponibilidade, integridade, confidencialidade e autenticidade previstas na IN nº 01/2008, em meio ao aumento das ameaças e tentativas de ataques contra as redes de instituições estratégicas do governo.

Primeiramente deve-se ficar claro que os envolvidos na estratégia de segurança devem trabalhar para o devido alinhamento com o objetivo institucional, e que as estratégias se iniciem da alta administração (Diretoria) seguindo o fluxo indicado na **Figura 33**.



**Figura 33 - A Governança de Segurança da Informação<sup>12</sup>.**

A consequência obtida para a organização depende das metas estabelecidas dentro da Governança de Segurança da Informação conforme o nível de maturidade desejado para os objetivos da Gestão de Riscos, com a redução do impacto nos ativos da informação; Gestão de Recursos, direcionar o uso do conhecimento e de infraestrutura de segurança; Gestão de Desempenho, medir e monitorar os processos de segurança da informação, reportar os resultados em favor do cumprimento dos objetivos; e Entrega de Valor, otimizando os investimentos em segurança da informação.

#### 3.1. Aplicabilidade do COBIT

<sup>12</sup> ITGI. 2006. **Information Security Governance**. [Online] 2006. [Citado em: 2012 de Maio de 19.] <<http://www.itgi.org/>>.

O COBIT é aplicável dentro de uma organização da APF relacionado a diferentes pontos de vista<sup>13</sup>, por exemplo: a) Gestão Executiva, orientação para obtenção de retorno sobre investimentos de acordo com os riscos inerentes a TI; b) Gestão de Negócio, auxílio para obtenção de garantias sobre o gerenciamento de serviços de TI; c) Gestão de TI, auxilia na provisão de serviços de TI adequados para suportar as estratégias de negócio, de forma controlada e gerenciada; d) Audidores, fornece o embasamento para suas conclusões e orientação para a gestão dos controles internos.

O COBIT possibilita a inserção de métricas que propiciam o acompanhamento dos requisitos de alinhamento estratégico, *compliance* e segurança da informação, fornecendo uma visão estratégica da segurança. O COBIT dá suporte aos Executivos e Alta Direção, na execução de suas atividades com o *Board Briefing on IT Governance, 2nd Edition*; aos Executivos de Negócios e Tecnologia utilizam diretrizes de gerenciamento e modelo de maturidade para medir a performance, comparar com outros modelos de gestão e efetuar aprimoramentos.

O COBIT fornece suporte para implementação de controles internos, conforme as leis e regulamentações. Processos de auditoria, monitoração, definição de níveis de maturidade são úteis para o cumprimento dos objetivos de segurança da informação por parte dos gestores das organizações.

Quatro processos do COBIT podem ser aplicados para controle diretamente na gestão de segurança da informação em órgãos da APF, são eles: PO 6 – Comunicar objetivos e direcionamentos gerenciais; PO 9 – Avaliar e gerenciar os Riscos de TI; DS 4 – Garantir a continuidade dos Serviços; DS 5 – Garantir a Segurança dos Sistemas.

De acordo com o COBIT<sup>14</sup>, as mudanças, manutenções e aplicação de patches de correção para a infraestrutura e aplicações de tecnologia devem ser formalmente gerenciadas e controladas. Isso evita que a instabilidade ou integridade incida em impactos na segurança da informação.

Pequenas ou grandes organizações da APF podem aplicar o COBIT para segurança cibernética desde que tenha definidos seus objetivos de negócios e estratégias de TI.

### 3.2. Aplicabilidade do ITIL

Consta no ITIL orientação para definir processos quanto ao gerenciamento da segurança da Informação, adotando uma abordagem relacionada à garantia dos critérios de confidencialidade, integridade e disponibilidade de dados, bem como a segurança dos componentes de hardware e software, documentações e procedimentos.

As práticas da ITIL prezam por uma forte abordagem de gestão, adaptável às características de cada organização, com ênfase nos aspectos tecnológicos e na sua integração com os requisitos do negócio (FERNANDES; ABREU, 2012).

---

<sup>13</sup> FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. Implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços. Rio de Janeiro: BRASPORT, 2012.

<sup>14</sup> ISACA. 2007. COBIT. [Online] 2007. [Citado em: 19 de setembro de 2012.] <<http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx>>.

A Gestão da Segurança da Informação por meio do ITIL considera o Gerenciamento de Nível de Serviço (ANS) entre os processos de negócio e de TI. Nessa visão há uma série de itens recomendados pelo ITIL passíveis de aplicação para melhoria da segurança da informação<sup>15</sup>. São eles: a) Catálogo de Serviços: a TI deve publicar na Organização um descritivo de seus serviços, com as respectivas condições, que atendem a cada requisito do Negócio; b) OLA's (Operational Level Agreement): deve ser estabelecido; é um SLA mais "enxuto", mas prevendo integralmente os serviços e suas condições, inclusive custos internos; c) UC's – Underpinning Contracts: são aqueles contratos estabelecidos com provedores externos, nos quais devem ser previstas todas as condições, incluindo bônus, penalidades, condições de saída, etc.; d) Banco de Dados dos ativos existentes e suas configurações atualizadas, incluindo software, hardware, documentação atualizada, procedimentos e classificação quanto à Segurança; e) Criação de um Service Desk como ponto focal de contato para todos os Usuários de TI; é a área "dona" de todos os incidentes e seu foco é a continuidade de serviço e manutenção do SLA; incluem-se aí os incidentes de Segurança; f) Gestão de Problemas: nessa área são estudados os incidentes, determinando sua relação, causas e medidas para evitá-los; essa abordagem permite detectar "brechas" de Segurança e deve prever forte documentação dos incidentes e soluções; g) Gestão de Mudanças: coordenam todas as mudanças em infraestrutura de TI, apoia-se na documentação dos incidentes e é responsável pela mudança.

O exame dos impactos que podem afetar a organização pode ser quantificado e qualificado com uso do ITIL. Nesse sentido, ele é considerado fundamental para: identificar os eventos que podem causar interrupções nos processos de negócios; avaliar os riscos e assim determinar o impacto das interrupções; e elaborar um plano estratégico que proporcione ou ajude a proporcionar a continuidade do negócio.

O Gerenciamento de Continuidade (PCN) dos serviços de TI previstos no ITIL suportam os processos de negócio da organização de acordo com o nível de maturidade ao qual a organização está submetida. A identificação dos riscos que uma organização da APF possa estar exposta ajuda na elaboração dos requisitos de disponibilidade dos serviços de TI e justificam os custos de investimentos. De acordo com Magalhães e Pinheiro (2007)<sup>16</sup>, tal gerenciamento deve recuperar o sistema de tecnologia em menor tempo possível dada as devidas prioridades. Os processos críticos da área de TI, bases para o negócio da organização, devem ser determinados inicialmente, bem como as medidas a serem adotadas para evitar a interrupção da continuidade dos serviços de TI. Os principais objetivos a serem atingidos pelo PCN relacionados com a segurança cibernética são: a) segurança de empregados; b) minimizar danos imediatos e perdas em uma situação de emergência; c) assegurar a restauração dos equipamentos o mais rápido possível; d) assegurar a rápida ativação dos processos de negócio críticos; e) fornecer conscientização e treinamento para as pessoas-chave para atividades de TI.

O Gerenciamento de Riscos do ITIL prevê cinco atividades que podem ser utilizados para prevenção de fatalidades de TI com a finalidade de controlar, identificar e analisar todos os riscos. A aplicação processo de Gerenciamento de Risco possibilita que haja uma preparação para circunstâncias os tis principalmente para as atividades críticas de uma organização da APF. As atividades são<sup>13</sup>: identificação dos riscos expostos; priorização

<sup>15</sup> INFOSEC COUNCIL. 2005. **Computerworld**. [Online] 2005. [Citado em: 20 de SETEMBRO de 2012.] <<http://computerworld.uol.com.br/gestao/2006/08/11/idgnoticia.2006-08-11.6447350724/>>.

<sup>16</sup> MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL**. São Paulo: Novatec, 2007.

quanto à probabilidade de concretizar; plano de ação para mitigação de riscos; divulgação e atualização de documentos; monitoramento e verificação do controle.

As vulnerabilidades de segurança cibernética podem ser tratadas pelo ITIL por meio de dois passos a serem adotados, nos quais deve ser aplicada uma escala de um a cinco em ordem crescente de probabilidade, considerando os custos de substituição e reparação. O primeiro passo é listar as vulnerabilidades influenciáveis na execução da contingência, ou outro é analisar todas as vulnerabilidades e considerar o que sobrevirá caso a ocorrência se confirme.

### 3.3. Aplicabilidade da ABNT NBR ISO/IEC 17799:2005<sup>17</sup>

Por se tratar de uma norma de prática para gestão da segurança da informação, a NBR ISO/IEC 17799 se aplica diretamente a organizações que utilizam a TI para alcançar os objetivos de controle, fazendo com que seja praticamente obrigatória para garantir a proteção dos ativos e significando um diferencial competitivo.

A aplicação de um sistema de gerenciamento de segurança da informação por meio da ISO/IEC 17799:2005 pode ser realizada em etapas cujo enfoque principal seja os aspectos críticos de segurança cibernética, que nas organizações podem ocorrer na parte física ou lógica. Deve ser considerada como um projeto de longa ou média duração, de acordo com a organização, e requer investimentos direcionados a esse fim.

As orientações da ISO/IEC 17799:2005 indicam o que deve ser feito em um sistema de gestão de segurança da informação, bem como a forma com que deve ser aplicada. Um diagnóstico para auxílio na percepção do nível de aderência de uma organização com a referida norma foi desenvolvido por Sêmola (2003)<sup>18</sup> por meio de um teste de conformidade.

De acordo com o TCU<sup>19</sup> a norma ISO/IEC 17799:2005 já é aplicada por órgãos da APF para segurança da informação por meio de sua incorporação a acordos e decisões normativas. Com a ISO são realizadas análises e avaliações para identificação dos requisitos e regras de segurança da informação que fazem parte de legislações, estatutos, regulamentações e cláusulas contratuais para apoiar e estabelecer as operações de órgãos e entidades da APF.

A ISO/IEC 17799:2005 prevê que a Política de Segurança da Informação deva ser alvo de comprometimento da alta direção e deva ser comunicada a todos os funcionários. Eis algumas das declarações contidas na referida ISO aplicáveis a APF: a) conceituação da segurança da informação, as metas globais, escopo e importância da segurança como mecanismo que habilita o compartilhamento de informações; b) declaração do comprometimento da direção, apoiando as metas e princípios da segurança, alinhado com os objetivos estratégicos do negócio; c) estrutura para estabelecer os objetivos de controle e os controles, incluindo a análise, avaliação e gerenciamento de riscos; d) breve explanação das políticas, princípios, normas e requisitos de conformidade da segurança da informação específico para a organização; e) definição de responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro de incidentes de segurança; f) referências à documentação que possam apoiar a política.

---

<sup>17</sup> ABNT—Associação Brasileira de Normas e Técnicas. Tecnologia da informação – Código de prática para a gestão da segurança da Informação. NBR ISO/IEC 17799.

<sup>18</sup> SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma visão Executiva. Rio de Janeiro: Campus, 2003. p. 156.

<sup>19</sup> TCU. 2008. Boas práticas em Segurança da Informação. Brasília: Tribunal de Contas da União, 2008.

A ISO/IEC 17799:2005 contém recomendações de segurança cibernética porquanto se refere a processamento, acesso, comunicações e gerenciamento das informações advindas de partes externas a organização. Convém que: a) a segurança dos recursos de processamento da informação e da informação da organização não seja reduzida pela introdução de produtos ou serviços oriundos de partes externas; b) qualquer acesso aos recursos de processamento da informação da organização e ao processamento e comunicação da informação por partes externas seja controlado; c) seja feita uma análise/avaliação dos riscos envolvidos para determinar as possíveis implicações na segurança e os controles necessários para trabalhar com partes externas que possa requerer acesso aos recursos de processamento da informação e à informação da organização, ou na obtenção e fornecimento de um produto e serviço de uma parte externa ou para ela; d) controles sejam acordados e definidos com a parte externa.

No que se refere à gestão de riscos, a ISO/IEC 17799:2005 prevê atividades coordenadas para direcionar e controlar a organização, fazendo com que haja análise, avaliação, tratamento, aceitação e comunicação dos riscos. Para cada risco identificado, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco deve ser tomada. As possíveis opções são: a) aplicar controles apropriados para reduzir os riscos; b) conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para a aceitação de risco; c) evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos; d) transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Para os riscos no qual a decisão de tratamento seja a de aplicar os controles apropriados, convém que esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos. A princípio, esses controles devem assegurar que os riscos sejam reduzidos a um nível aceitável, levando-se em conta: a) os requisitos e restrições de legislações e regulamentações nacionais e internacionais; b) os objetivos organizacionais; c) os requisitos e restrições operacionais; d) custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da organização; e) a necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Os objetivos de controles apropriados para uma organização da APF no que se refere a segurança cibernética devem ser selecionados de acordo com a análise dos riscos a que a organização pública possa estar sujeita. Isso determinará a sua real necessidade, viabilidade, relação custo benefício para, a partir de então, os controles serem implantados.

### **3.4. Aplicabilidade do PMBOK**

O PMBOK pode ser usado para definir os procedimentos a serem adotados em um projeto de implantação da segurança da informação, destinado a controlar o acesso a informações críticas contra modificação, destruição e utilização indevida ou não autorizada. A formalização da metodologia do PMBOK na APF ocorre em projetos específicos, como por exemplo, a padronização da documentação, implantação ferramentas e técnicas utilizadas, e na criação de indicadores para monitoramento. A aplicação dos PMBOK deve estar adaptada e integrada aos princípios da Governança de TI em todas as suas áreas do conhecimento.

Segundo Brito (2009)<sup>20</sup> “As áreas de conhecimento, as métricas de avaliação e principalmente a documentação gerada pelas lições aprendidas no projeto implementação do SGSIC são fatores críticos de sucesso para a criação da cultura de Gestão da Segurança da Informação e Comunicação”.

O PMBOK também pode ser aplicado total ou parcialmente, fazendo uso de ferramentas de gerenciamento de projetos existentes. Tudo isso significa dar a consistência necessária, pois deverão ser feitas adaptações em função do tipo, porte e riscos da organização (FERNANDES; ABREU, 2012)<sup>21</sup>.

Normalmente há consideráveis resistências dentro das organizações na aplicação de metodologias de gerenciamento de projetos. Um dos fatores mais importantes para se alcançar o objetivo é um grande comprometimento da alta administração e gerentes de TI, a fim de superar as dificuldades naturais, principalmente àquelas relacionadas com a segurança cibernética.

### **3.5. Aplicação da Norma ISO 17799 com os Modelos COBIT e ITIL**

A relação entre a norma ISO 17799 com os modelos COBIT e ITIL aplicados ao tema da segurança cibernética contribui de modo mais eficaz na diminuição dos riscos relacionados com o uso da tecnologia da informação no espaço cibernético e para a análise dos indicadores.

A Governança de segurança da Informação de uma organização pode tirar proveito em níveis organizacional, tático e estratégico dos objetivos de controle abordados pelo modelo COBIT e pela norma ISO 17799, bem como os referenciados pelos processos abordados pelo modelo ITIL (BERNARDES; MOREIRA, 2005)<sup>22</sup>.

Para a implementação da defesa cibernética na APF dentro dos requisitos deste trabalho, a Tabela 9 propõe a utilização do COBIT e ITIL, tendo por base a norma ISO 17799 que detalha o gerenciamento de segurança computacional. Nesse processo de implantação pode ser utilizado o gerenciamento de projeto PMBOK. Para os serviços de tecnologia oferecidos pela organização, o COBIT pode aplicar seus controles em alto nível adaptados às práticas de segurança computacional, dando uma maior abrangência à ISO 17799 que possui seus controles de forma mais detalhada. Nisso deve ainda ser incluídas a avaliação do nível de maturidade e os processos de melhoria contínua para cada um dos controles da ISO.

Posteriormente ao fornecimento dos controles pelo COBIT e ISO 17799, a ITIL detalha o que deverá ser feito em nível operacional e tático, e quem será o seu responsável. No nível estratégico da organização, é realizada a análise de risco nas situações em que serão definidos os requisitos a serem implementados, o modelo de maturidade estipulado e as necessidades de investimentos na execução do planejamento (BERNARDES; MOREIRA, 2005).

---

<sup>20</sup> BRITO, Antonio Carlos Pereira de. Estudo do Gerenciamento de Projeto Baseado no PMBOK para a Implantação da Gestão de Segurança da Informação e Comunicação na Administração Pública Federal. Brasília: UNB MONOGRAFIA, 2009.

<sup>21</sup> FERNANDES, Aguinaldo Aragon; Abreu, Vladimir Ferraz de. Implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços. Rio de Janeiro: BRASPORT, 2012.

<sup>22</sup> BERNARDES, Mauro Cesar; MOREIRA, Edson dos Santos. Artigo científico: um modelo para inclusão da governança da segurança da informação no escopo da governança organizacional, v.1, n.1, p. 1-10, out. 2005. Disponível em: <ftp://linorg.cirp.usp.br/pub1/SSI/SSI2005/artigos.html>. Acesso em: 28 maio 2012.

**Tabela 3 - A relação entre a norma ISO 17799 com os modelos COBIT e ITIL aplicados ao tema da segurança cibernética**

---	OPERACIONAL	TÁTICO	ESTRATÉGICO
<b>CONTROLES</b>	- ISO 17799 - COBIT: Entrega e Suporte - COBIT: Aquisição e Implementação	- ISO 17799 - COBIT: Entrega e Suporte	- ISO 1799 - Análise de Risco - COBIT: Auditoria - COBIT: Monitoramento - COBIT: Planej. e Organização
<b>PESSOAS</b>	-ITIL: Suporte a Serviços (adaptado)	- ITIL: Entrega de Serviços (expandido)	- COBIT: Auditoria - COBIT: monitoramento
<b>PROCESSOS</b>	-ITIL: Suporte a Serviços (adaptado)	- ITIL: Entrega de Serviços (expandido)	- COBIT: Auditoria - COBIT: Monitoramento

#### 4. Conclusão

A proposta deste trabalho referente à Governança de TI para segurança cibernética da Administração Pública Federal atinge principalmente a estrutura de decisão dos sistemas de informações gerenciais. Dessa forma, ela pode ser aplicada pela alta gerência de órgãos e entidades públicas, inserindo-se desta forma na realidade da APF.

Sabe-se que há dificuldades para tomada de decisões relacionadas a negócios e ao gerenciamento de segurança cibernética, quando se trabalha com grandes volumes de dados. Há de ser dada atenção ao fato de que a preocupação com a segurança das informações não pode servir de escusas à necessária transparência dos atos públicos. A motivação para utilização desta proposta consiste no que pode ser extraído com mais relevância sobre as principais referências da área de Governança de TI.

Antes das propostas apresentadas, foi feito um mapeamento da Segurança da Informação na APF, levando-se em consideração as dimensões relevantes para o alinhamento estratégico entre a segurança cibernética com o negócio da organização pública. O desafio de harmonizar as dimensões onde ocorre influência da cultura de compartilhamento de informações, da socialização, da transparência, da criação de conhecimento, e juntamente com o que se refere a proteção, segurança, confidencialidade, e privacidade. Por causa dessa abrangência, foram elencados os controles, processos, pessoas e tecnologias de acordo com os níveis de decisão: estratégico, tático e operacional. Nesse mapeamento, através dos levantamentos realizados pelo Tribunal de Contas da União, foi possível concluir que o país carece de uma apropriada gestão estratégica do espaço cibernético e da necessidade de segurança desse espaço cada vez mais relacionado com a segurança da própria Nação.

Com o aprofundamento dos estudos, verificou-se que a segurança cibernética é discutida amplamente pelos principais governos mundiais e que há uma necessidade urgente e constante da construção de uma doutrina que garanta uma segurança efetiva das infraestruturas críticas nacionais. Com isso, foram reconhecidas a dificuldade e a grandeza da tarefa de estabelecer uma Governança com esse propósito. Não existem modelos a serem seguidos, são poucas as nações que se debruçaram sobre o tema, e aquelas que o fizeram ainda estão construindo seus referenciais teóricos e práticos<sup>23</sup>. A tarefa deve ser construída com base em um conhecimento aprofundado das características particulares do Estado e da Sociedade. Assim, a busca pela proteção do Espaço Cibernético, dos ativos de informação e

<sup>23</sup> Revista Desafios Estratégicos para Segurança Cibernética – Brasília, 2011. Disponível em: <<http://www.sae.gov.br>>.



das infraestruturas críticas do país, por meio deste trabalho não possui a pretensão de esgotar o assunto.

O estímulo primordial é contribuir colaborativamente por meio de propostas com a visão técnico-estratégica que vem sendo adotada pelo Governo com o apoio de diversos especialistas de diferentes órgãos da APF e efetivada na missão do GSIPR.

Foram extraídos dos modelos COBIT, ITIL, NBR ISO/IEC 17799:2005 e PMBOK as informações vislumbradas como mais pertinentes para as aplicabilidades propostas. A combinação desses modelos Governança de Segurança da Informação permitiu potencializar as medidas que elas oferecem, com o intuito de identificar respostas as seguintes indagações: o que (controle), quem (pessoas), como (processos) e com que recurso (ferramentas tecnológicas) traçar as estratégias para defesa cibernética.

A possibilidade do aproveitamento de que tais propostas apresentadas fortaleçam a segurança das informações permite idealizar uma Administração Pública com processos de negócios e controles eficazes, em que os recursos públicos estejam protegidos de desperdícios, desvios, fraudes e ataques cibernéticos.

## Referências

- ABNT–Associação Brasileira de Normas e Técnicas. **Tecnologia da informação – Código de prática para a gestão da segurança da Informação**. NBR ISO/IEC 17799.
- BERNARDES, Mauro Cesar; MOREIRA, Edson dos Santos. Artigo científico: **Um modelo para inclusão da governança da segurança da informação no escopo da governança organizacional**, v.1, n.1, p. 1-10, out. 2005. Disponível em:<ftp://linorg.cirp.usp.br/pub1/SSI/SSI2005/artigos.html>. Acesso em: 28 maio 2012.
- BRASIL. Instrução Normativa de 13 de junho de 2008. **Disciplina a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta**. Diário oficial da União, n. 115, 18 jun. 2008.
- BRASIL. **Portaria n.º. 34, de 05 de agosto de 2009**. Diário Oficial da República Federativa do Brasil, Brasília, 06 ago 2009.
- BRASIL, Tribunal de Contas da União (TCU). **Levantamento de governança de TI**. TCU. Brasília : TCU, 2010. p. 49. Relator Ministro Aroldo Cedraz – Disponível em: <www.tcu.gov.br/fiscalizacaoti>.
- BRASIL. Decreto n.º 6.703, de 18 de dezembro de 2008. Aprova a **Estratégia Nacional de Defesa**, e dá outras providências. Diário Oficial da União, Poder Executivo, Brasília, DF, 19 dez. 2008.
- BRITO, Antônio Carlos Pereira de. Estudo do Gerenciamento de Projeto Baseado no PMBOK para a Implantação da Gestão de Segurança da Informação e Comunicação na Administração Pública Federal. Brasília: UNB MONOGRAFIA, 2009.
- FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI - da Estratégia à Gestão de Processos e Serviços**. Rio de Janeiro: BRASPORT, 2012.
- INFOSEC COUNCIL. 2005. **Computerworld**. [Online] 2005. <http://computerworld.uol.com.br/gestao/2006/08/11/idgnoticia.2006-08-11.6447350724/>.
- ISACA. 2007. **COBIT**. [Online] 2007. [Citado em: 19 de setembro de 2012.] <http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx>.

- ITGI. 2006. **Information Security Governance**. [Online] 2006. [Citado em: 2012 de Maio de 19.] <<http://www.itgi.org/>>.
- MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL**. São Paulo: Novatec, 2007.
- MANDARINO JUNIOR, R. **Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro**. 2009. Monografia (especialização). Universidade de Brasília (UnB). Departamento de Ciência da Computação - DCE: Brasília. Jun. 2009. p. 29.
- MANDARINO JUNIOR, Raphael. 2010. **Segurança e Defesa do Espaço Cibernético Brasileiro**. Recife: CUBZAC, 2010. p. 182.
- Organization for Economic Co-Operation and Development (OECD) - **Guidelines for the Security of Information Systems and Networks: Towards a culture of security**. (Adopted as a Recommendation of the OECD Council at its 1037<sup>th</sup> Session on 25 July 2002). Paris: OECD. 2002. 28p
- OLIVEIRA, João Roberto de. **Sistema de Segurança e Defesa Cibernética Nacional**. Desafios Estratégicos. 2011, p. 216.
- SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão Executiva**. Rio de Janeiro: Campus, 2003. p. 156.
- TCU. 2008. **Boas práticas em Segurança da Informação**. Brasília: Tribunal de Contas da União, 2008.