**UNIVERSIDADE DE BRASÍLIA**
**FACULDADE DE TECNOLOGIA**
**DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

# ESTUDO E PROPOSTA PARA IMPLANTAÇÃO DA NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO SENADO FEDERAL

**ALCIDES RIBEIRO VIEIRA MAGALHÃES**

**e**

**DEVAIR SEBASTIÃO NUNES**

**ORIENTADOR**

**ANDERSON CLAYTON ALVES NASCIMENTO**

**MONOGRAFIA DE ESPECIALIZAÇÃO**

**PUBLICAÇÃO: UNB.LABREDES.MFE.005/2006**

**BRASÍLIA / DF: AGOSTO/2006**

# UNIVERSIDADE DE BRASÍLIA
# FACULDADE DE TECNOLOGIA
# DEPARTAMENTO DE ENGENHARIA ELÉTRICA

## ESTUDO E PROPOSTA PARA IMPLANTAÇÃO DA NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO SENADO FEDERAL


## ALCIDES RIBEIRO VIEIRA MAGALHÃES

**e**

## DEVAIR SEBASTIÃO NUNES


MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA.

APROVADA POR:

---

**ANDERSON CLAYTON ALVES NASCIMENTO, Phd, UnB**
**(ORIENTADOR)**

---

**VERA PARUCKER HARGER, Especialista, UFRJ**
**(EXAMINADORA)**

---

**ODACY LUIZ TIMM JR, MS OM**
**(EXAMINADOR EXTERNO)**

**DATA: BRASÍLIA/DF, 28 DE AGOSTO DE 2006.**

## FICHA CATALOGRÁFICA

MAGALHÃES, ALCIDES RIBEIRO VIEIRA e NUNES, DEVAIR SEBASTIÃO. Estudo e Proposta para Implantação da Nova Política de Segurança da Informação do Senado Federal [Distrito Federal] 2006. (xx), (71) p., 297 mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2006).

Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Governo 2. Poder Legislativo
3. Política de Segurança da Informação

I. ENE/FT/UnB. II. Título (Série)

## REFERÊNCIA BIBLIOGRÁFICA

MAGALHÃES, A. R. V. (2006) e NUNES, D. S. (2006) Estudo e Proposta para Implantação da Nova Política de Segurança da Informação do Senado Federal. Monografia de Especialização, Publicação UNB.LABREDES.MFE.005/2006. Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, (71)p.

## CESSÃO DE DIREITOS

NOME DO AUTOR: Alcides Ribeiro V. Magalhães e Devair Sebastião Nunes
TÍTULO DA DISSERTAÇÃO: Estudo e Proposta para Implantação da Nova Política de Segurança da Informação do Senado Federal
GRAU/ANO: Especialista/2006.

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Monografia de Especialização e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte desta dissertação de especialização pode ser reproduzida sem a autorização por escrito do autor.

Alcides Ribeiro Vieira Magalhães
SQS 311 Bloco C – Apto 602 – Asa Sul
CEP 70364-030 – Brasília – DF – Brasil

Devair Sebastião Nunes
SQSW 305 Bloco A – Apto 305 – Setor Sudoeste
CEP 70673-421 – Cruzeiro – DF – Brasil

# DEDICATÓRIA

Dedico este trabalho de especialização ao meu pai Professor Almo Saturnino Vieira Magalhães, que desde a minha infância me educou, me corrigiu e me estimulou a estudar, a me aperfeiçoar e a crescer como ser humano e como profissional a fim de que eu pudesse tornar-me útil aos meus concidadãos e que pudesse me dedicar à melhoria das condições de vida do povo brasileiro, e à minha mãe Rachel de Mello R. V. Magalhães que através de sua firme vontade não permitiu que eu trilhasse caminhos errados, direcionando minha vida à responsabilidade e à dignidade. A todos vocês dois, amados pais, meu mais carinhoso obrigado!

Alcides Ribeiro Vieira Magalhães

Dedico este trabalho de especialização aos meus antepassados, que vieram a este país contra sua vontade, mas mesmo assim serviram ao engrandecimento do Brasil, e também aos meus pais que, apesar do pouco estudo que tiveram não mediram esforços para que seu filho sentisse orgulho de sua origem e conseguisse sucesso em sua vida. A todos vocês, meu mais sincero muito obrigado!

Devair Sebastião Nunes

# AGRADECIMENTOS

Ao nosso orientador Professor ANDERSON CLAYTON ALVES NASCIMENTO pelo apoio, incentivo, dedicação e amizade essenciais para o desenvolvimento deste trabalho.

À Professora VERA PARUCKER HARGER co-orientadora deste trabalho, que, apenas por razões de regulamentação, não pode ser registrado formalmente como tal.

Ao Professor ODACYR LUIZ TIMM JR. pela eficiente coordenação do curso e pela criação de um ambiente apropriado ao aprendizado.

Às empresas e instituições: Aker Security Solutions, BID - Banco Interamericano de Desenvolvimento, Biblioteca do Congresso dos EUA, BrasilTelecom, EMBRAPA - Empresa Brasileira de Pesquisa Agropecuária, IBM, Ministério da Agricultura, Ministério da Ciência e Tecnologia, Oracle, POLITEC, PMI – Capítulo DF, Secretaria de Tecnologia da Informação do Distrito Federal, SERPRO - Serviço Federal de Processamento de Dados, SISCO, SYBASE, SUN e Universidade George Washington que nos concederam palestras esclarecedoras sobre os diversos temas tratados durante o curso.

Agradecimento especial de Alcides Ribeiro Vieira Magalhães todos os colegas servidores da Subsecretaria de Infra-estrutura Tecnológica do Prodasen, especialmente a Pedro Enéas Mascarenhas, Ricardo Camargo, José Salo Reiman, Eduardo Ferraz, Marcelo Abrantes, Marco Cícero Gouveia e a Arnaldo Moreira da Silva que foram bastante gentis e solícitos na colaboração com o nosso grupo trazendo excelentes sugestões e recomendações. A todos, o meu muito obrigado!

Agradecimento especial de Devair Sebastião Nunes aos colegas do Prodasen Rui Oscar Dias Janiques, Edward Cattete Pinheiro Filho e Aníbal Moreira Junior que desde o início sempre apoiaram a realização deste estudo, e a todos os colegas da SSDAS/SSS que sempre prestaram apoio nas atividades diárias.

O presente trabalho foi realizado com o apoio institucional e financeiro da Secretaria Especial de Informática do Senado Federal – Prodasen, órgão responsável pela gestão da Tecnologia da Informação no Senado Federal.

# Estudo e proposta para implantação da Nova Política de Segurança da Informação do Senado Federal

## RESUMO

O trabalho apresentado nesta dissertação faz um estudo do ambiente do Senado Federal e das Normas ABNT NBR/ISO 17799:2005 e 27000:2006 com o objetivo de lançar as bases para a implementação de uma Nova Política de Segurança da Informação para o Senado Federal seguindo princípios atualizados nesta área de conhecimento.

A metodologia utilizada foi: entrevistas com técnicos da Secretaria Especial de Informática do Senado Federal – Prodasen, estudo das normas citadas, avaliação da legislação vigente e pesquisa em bibliografia especializada.

Ao final deste trabalho apresentamos uma minuta de Política de Segurança da Informação para o Senado Federal e ações imediatas recomendadas ao Prodasen para a preparação e adequação à Nova Política de Segurança da Informação.

# Study and proposal for implantation of a New Information Security Policy to Brazilian Federal Senate

## ABSTRACT

This dissertation presents a study of the Brazilian Federal Senate environment and ABNT NBR/ISO 17799:2005 and 27000:2006 Standards in order to launch the bases for the implementation of a New Information Security Policy for the Brazilian Federal Senate in accordance with up to date principles from this area of knowledge.

The methodology used to gather data consisted of interviews with technicians from Secretaria Especial de Informática do Senado Federal – Prodasen (Brazilian Federal Senate's IT Special Bureau), study of the Standards cited above, evaluation of the current law and research in specialized bibliography.

At the end of this work we present a draft of an Information Security Policy for the Brazilian Federal Senate and suggest immediate actions in order to prepare and adequate the Prodasen to follow the new patterns.

# ÍNDICE

Item Página

# ÍNDICE DE TABELAS

Tabela Página

# ÍNDICE DE FIGURAS

Figura Página

## ÍNDICE DE ABREVIAÇÕES

| | | |
|---|---|---|
| GB | – | Giga Byte |
| FTP | – | File Transfer Protocol |
| HD | – | Hard Disck |
| PC | – | Personal Computer |
| PISI | – | Plano de Implementação da Segurança da Informação |
| PSI | – | Política de Segurança da Informação |
| ROI | – | Return Of Investment |
| TI | – | Tecnologia da Informação |
| USB | – | Universal Serial Bus |
| VPN | – | Virtual Private Network |
| WEB | – | World Wide Web |

# 1. INTRODUÇÃO

A Informação é, nos dias atuais, o bem mais valioso que a sociedade possui, e se não estiver adequadamente gerida poderá vir a servir de arma para agentes nocivos às pessoas, organizações e países. Dentro desse cenário o Senado Federal deve promover uma Política de Segurança da Informação a fim de resguardar-se de ameaças contra seus ativos que, se concretizadas, podem causar grande prejuízo ao país.

No contexto da tecnologia verificamos nos últimos anos um vertiginoso avanço nas facilidades de produção, armazenamento e distribuição da informação. Hoje é possível em um dispositivo de apenas 2,5cm x 9,2cm e com somente 18g armazenar cerca de 64GB de informação que equivalem, grosso modo, a mais de 60.000 páginas de texto em MS-Word! Observamos ainda uma popularização do uso de câmaras fotográficas digitais e da telefonia móvel, que permitem a uma pessoa capturar uma informação e transmiti-la em segundos, não deixando nenhum vestígio do fato. Somando-se isto tudo à popularização dos recursos computacionais, podemos verificar um grande aumento no número de vulnerabilidades a que as organizações estão sujeitas. Assim, o risco de violação da segurança da informação é enorme e ações devem ser tomadas para que os ativos do Senado Federal estejam protegidos.

## 1.1. POR QUE UMA NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA O SENADO FEDERAL?

Tendo em vista o avanço tecnológico, as mudanças no ambiente externo e no ambiente interno do Senado Federal com alteração da estrutura organizacional, o aperfeiçoamento no modelo da gestão pública e ainda o surgimento de conceitos atualizados sobre a segurança da informação, tornou-se necessária uma revisão profunda da Política da Segurança da Informação do Senado Federal.

Na gestão atual, cada unidade organizacional do Senado Federal implementa sua política própria de Segurança da Informação, gerando brechas que devem ser corrigidas pela adoção de uma visão corporativa do tema. Devido a essa necessidade de uniformizar as ações de segurança da informação viemos, neste trabalho, oferecer um estudo para a implementação de uma Nova Política de Segurança da informação para o Senado Federal.

## 1.2. O QUE É A SEGURANÇA DA INFORMAÇÃO?

Segundo a norma ABNT NBR ISO/IEC 17799:2005 [1] a informação é um ativo essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é particularmente importante em um ambiente altamente interconectado como é o caso do Senado Federal. Neste ambiente conectado o número e a variedade de ameaças bem como as vulnerabilidades vêm crescendo muito, exigindo cada vez mais a atenção dos gestores e mais recursos para mitigar o dissabor de ver, ou pior, não ver a preciosa informação ser levada por agentes maliciosos.

Na norma ABNT NBR ISO/IEC 17799:2005, Introdução, página ix temos:

> *"A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."*

No caso do Senado Federal o negócio é **legislar,** de forma que a visão comum sobre continuidade do negócio, risco do negócio, maximização do investimento e oportunidades do negócio não se aplicam diretamente. Mas nem por isso a segurança é menos importante. Muito pelo contrário, a manutenção eficaz da segurança da informação no Senado Federal permitirá às outras organizações do país atuar tranqüilas para obter os benefícios do negócio que operam. Por este prisma, a Segurança da Informação do Senado Federal deveria ser tratada como tema de Segurança Nacional, tão alto será o preço a pagar por falhas que venham a ocorrer nesta área.

Ainda citando a norma ABNT NBR ISO/IEC 17799:2005, Introdução, página ix encontramos:

> *"A segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde 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”.*

Seguindo essas orientações iremos apresentar o estudo e a proposta de implantação de uma Nova Política de Informação para o Senado Federal que julgamos ser um primeiro subsídio para a renovação do assunto nesta casa.

## 1.3. POR QUE A SEGURANÇA DA INFORMAÇÃO É NECESSÁRIA?

Para o Senado Federal a segurança da informação é uma atividade essencial para assegurar o eficaz desempenho de suas atividades, atender aos requisitos legais, manter a imagem da instituição perante a população e dar suporte à estabilidade ao Legislativo Federal, garantindo tranqüilidade à nação.

A Segurança da Informação deve manter as seguintes propriedades da Informação:

**Tabela 1.1 - Propriedades da Informação.**

| Propriedade | Descrição |
|---|---|
| Autenticidade | É a certeza absoluta de que a informação provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo. |
| Confidencialidade | É a certeza de que a informação não estará disponível nem revelada a indivíduos, entidades ou processos não autorizados. |
| Disponibilidade | A informação deverá estar acessível e utilizável sob demanda por uma entidade autorizada sempre que requisitada. |
| Integridade | É a salvaguarda da exatidão e completeza da informação. |
| Legalidade | Esta propriedade deve garantir que toda informação deverá ser |

| Propriedade | Descrição |
|---|---|
| | manuseada, armazenada, transportada e descartada seguindo os preceitos legais vigentes. |
| Não-repúdio | É a garantia que o emissor de uma informação ou a pessoa que executou determinado manuseio da mesma não possa posteriormente negar sua autoria. |

As informações que são tratadas nesta instituição são continuamente expostas a diversos tipos de ameaças tais como fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio, inundação e até mesmo terrorismo, entre outras ameaças comuns às organizações.

A tecnologia, sozinha, é insuficiente para implementar a segurança da informação, a qual deve ser garantida por uma gestão e procedimentos corretos e atuais.

A gestão da segurança da informação requer a participação de todas as pessoas da organização. Isto deverá ser garantido através da aplicação de uma Política de Segurança da Informação que não deixe de fora nenhum agente, quer seja da casa, quer seja terceiro.

Ressalta-se que para a aplicação eficaz dos novos conceitos da Política de Segurança poderá ser necessário o auxílio de uma consultoria externa especializada que, dentre as atividades que executará, deverá organizar treinamento específico para os agentes da segurança da informação nos diversos níveis da administração do Senado Federal.

## 1.4. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

Existem três fontes principais de requisitos de segurança da informação:

1. Análise de riscos;
2. Legislação;
3. Conjunto de princípios, objetivos e requisitos do negócio.

De acordo com a análise a ser feita, outros requisitos importantes poderão ser encontrados. Neste estudo, todavia, são apresentados basicamente os sugeridos pela norma ISO 17799. A instituição deverá rever continuamente os requisitos para manter atualizada suas ações. Para isso deverá contar com uma estrutura organizacional dedicada que apresentaremos neste estudo.

Cabe ressaltar que, no item 2 apresentado acima, para o Senado Federal ocorre uma singular peculiaridade: O Senado Federal é, juntamente com a Câmara dos Deputados, a principal instituição encarregada de elaborar a legislação do país, embora existam outras fontes de legislação no Brasil. Isto traz à casa uma situação que lhe permite, quando desejar, alterar a legislação para se adequar aos fatos ou impor uma determinada forma de atuação a si própria ou a terceiros. Esta liberdade de atuação, no nosso entender, deverá ser utilizada ao máximo para garantir os objetivos da segurança almejados. Os únicos limites para esta atuação deverão ser os princípios da ética, da moral e da justiça.

## 1.5. FATORES CRÍTICOS PARA O SUCESSO

Seguindo orientação da norma ISO 17799, são fatores críticos para o sucesso da implantação da segurança da informação:

1. Política de segurança da informação, objetivos e atividades de acordo com o objetivo do negócio. No caso do Senado Federal, legislar.

2. Comprometimento e apoio visível de todos os níveis gerenciais.

3. Uma abordagem e uma estrutura organizacional para garantir a implantação, manutenção, monitoramento e melhoria da segurança da informação consistente com a cultura da casa.

4. Bom entendimento dos requisitos de segurança da informação.

5. Divulgação eficiente da segurança da informação para todos os envolvidos (funcionários, fornecedores, etc.) para alcançar a conscientização necessária.

6. Provisão de recursos para as atividades de gestão de segurança da informação.

7. Treinamento e educação adequados.

8. Estabelecer um eficiente processo de gestão de incidentes de segurança da informação.

9. Avaliar o desempenho da gestão da segurança da informação através de métricas e metas estabelecidas.

10. Criar um mecanismo para a obtenção de sugestões para a melhoria da segurança da informação.

## 1.6. IMPLEMENTANDO A SEGURANÇA DA INFORMAÇÃO

Os principais controles para a implementação da segurança da informação são:

1. Atribuição de responsabilidades para a segurança da informação;

2. Conscientização e educação em segurança da informação;

3. Direitos e deveres legais;

4. Documento da Política de Segurança da informação;

5. Execução correta dos sistemas de software e hardware;

6. Gestão de continuidade dos negócios. No caso, atividades Legislativa e Administrativa do Senado Federal.

7. Gestão de incidentes de segurança;

8. Gestão de vulnerabilidades;

9. Proteção de dados e privacidade de informações pessoais;

10. Proteção de registros organizacionais;

## 1.7. BARREIRAS DA SEGURANÇA

Diante da amplitude e complexidade da aplicação da segurança da informação, segundo Marcos Sêmola [2],*in* Gestão da Segurança da Informação, pág. 52-55, a aplicação

da segurança da informação deve ser por níveis denominados Barreiras da Segurança. Essas barreiras são em número de seis. A saber:

**Tabela 1.2 - Barreiras da Segurança.**

| Barreira | Descrição |
|---|---|
| 1 - Desencorajar | Cumpre o papel de desencorajar as ameaças. As ameaças podem ser desestimuladas por efeito de mecanismos físicos, tecnológicos e humanos. |
| 2 - Dificultar | Completa a ação anterior através de medidas que irão dificultar o acesso indevido. |
| 3 - Discriminar | Conjunto de recursos que permitem identificar e gerir os acessos, definindo perfis e autorizando permissões. |
| 4 - Detectar | Conjunto de mecanismos que sinalizem, alertem e instrumentem os gestores da segurança na detecção de situações de risco ou violação das normas estabelecidas. Inclui mecanismos de auditoria. |
| 5 - Deter | Essa barreira deve acionar mecanismos que impeçam danos aos ativos da organização uma vez que as demais barreiras falharam. |
| 6 - Diagnosticar | Esta barreira atua em conjunto com todas as demais, permitindo o contínuo aprimoramento dos mecanismos de segurança da informação. |

A implementação das Barreiras da Segurança deve ser feita através de um correto diagnóstico das ameaças e vulnerabilidades mediante o uso de uma metodologia e

instrumentos adequados. Caso contrário a implementação das barreiras será ineficaz fornecendo uma falsa sensação de segurança que colocará o negócio e os ativos em risco.

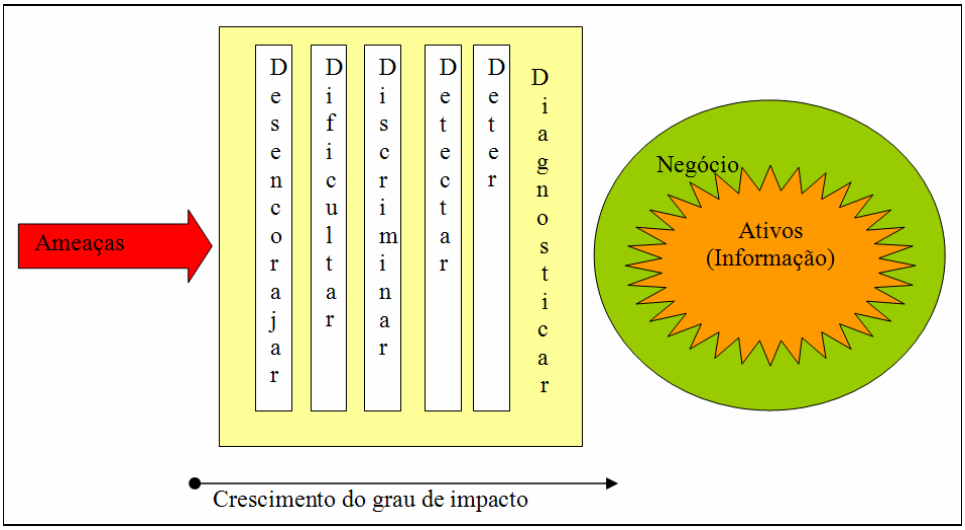



**Figura 1.1 - Diagrama representativo das barreiras da segurança.**

O correto diagnóstico deverá levar em conta a ameaça, o risco sobre o ativo e o custo da implementação das barreiras. Particularmente no caso do Senado Federal o custo deverá ser considerar não só o dano à organização, mas também à sociedade que representa.

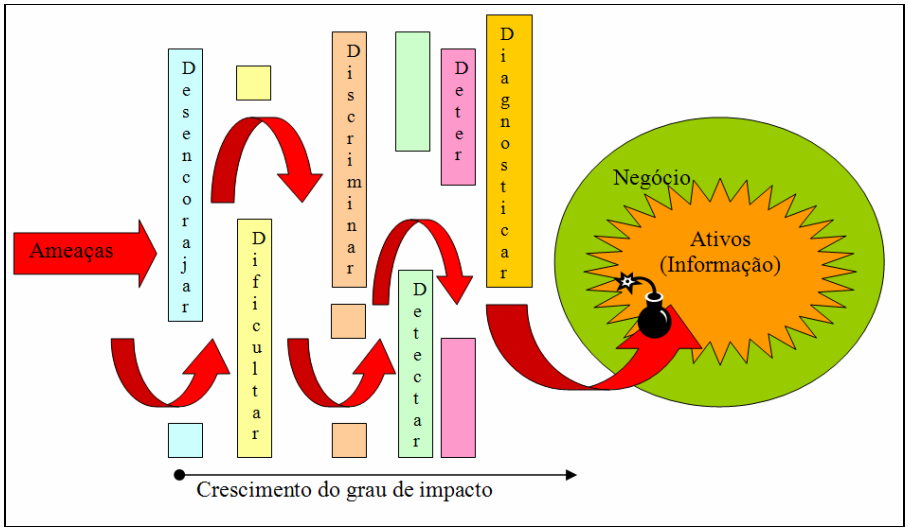



**Figura 1.2 - Ilustração simbólica das barreiras da segurança orientada por diagnóstico inadequado.**

## 1.8. ANÁLISE DE CONTEXTO DA SEGURANÇA DA INFORMAÇÃO.

É impossível operar com risco ZERO. Embora exista o desejo de que toda ameaça seja totalmente evitada ao serem adotados mecanismos de controle isto de fato não ocorre. Isto é assim porque são muitas as variáveis que envolvem cada risco e todas estão em constante mutação. A despeito disto, ações adequadas poderão colocar os riscos dentro de um nível aceitável.

Na análise de risco da segurança da informação temos que avaliar a situação por três ângulos diferentes: a visão da tecnologia, a visão dos processos e a visão das pessoas. Toda vulnerabilidade e risco decorrerão de pelo menos uma destas três facetas, mas como essas facetas estão intrinsecamente ligadas, é impossível impedir que o problema de uma não reflita em outra. Assim, as ações para mitigar o problema, de um modo geral, deverão ser aplicadas em todas as facetas onde o problema for detectado. Por exemplo: para evitar um ataque de vírus deverão ser tomadas ações no aspecto tecnológico – utilização de software antivírus; no aspecto dos processos – atualização periódica e; no aspecto humano – o usuário deve ser instruído para alertar prováveis problemas decorrentes de um ataque de vírus e a não desativar a proteção do software antivírus instalada. Porém, como falamos anteriormente, nenhuma das facetas é estática. Todas estão se modificando de instante a instante gerando um universo de problemas altamente complexo e volátil. Novos vírus são produzidos diariamente e novos softwares de proteção estão continuamente sendo desenvolvidos; a equipe de trabalho está sendo renovada e novas rotinas de trabalho estão sendo adotadas. Devemos ainda considerar que a tentativa de conter todos os riscos e vulnerabilidades poderá gerar efeitos colaterais que poderão impedir a eficiência da organização devido a um alto nível de burocratização, o que gerará a insatisfação dos colaboradores e, no caso do Senado Federal, da sociedade. No exemplo dado, um micro invulnerável a ataque de vírus é aquele que não está conectado à rede e que não possui dispositivos de acesso tais como unidades de disquetes, portas USB e unidades de CD; tal micro é pouca coisa melhor que uma máquina de escrever elétrica e, portanto, indesejável para o usuário.

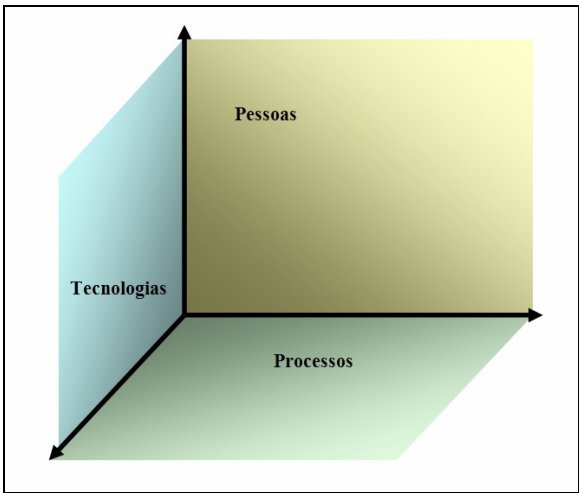



**Figura 1.3 -Visões para a análise da Segurança da Informação.**

De todas as visões a mais vulnerável de todas é a faceta humana. Todo ser humano tem uma maneira própria de interpretar o ambiente onde vive e daí decorre que haverá tantas maneiras diferentes de lidar com uma situação quantas forem as pessoas envolvidas. Cabe à gerência prover ações tais como a aplicação de normas de atuação e treinamentos contínuos para minimizar os problemas que surgirão nesta faceta.

## 1.9. CICLO DE VIDA DA INFORMAÇÃO

Independente da forma como a informação é representada, seja papel, bits, filmes, etc. toda informação passa por quatro momentos para os quais ações de segurança deverão ser adotadas. A tabela a seguir mostra os momentos do ciclo de vida da informação.

**Tabela 1.3 - Ciclo de Vida da Informação.**

| Momento | Descrição |
|---|---|
| Manuseio | Momento em que a informação é criada e manipulada.<br>Exemplos:<br>• Elaboração de uma minuta de relatório à mão.<br>• Digitação em um processador de textos. |

| Momento | Descrição |
|---|---|
| Armazenamento | Momento em que a informação é armazenada, independentemente do meio em que é feita.<br>Exemplos:<br>• Banco de dados.<br>• Disquete.<br>• *Pen drive*.<br>• Cofres.<br>• Arquivos de metal. |
| Transporte | Momento em que a informação é transportada, independentemente do meio em que é feita. Exemplos:<br>• Correio.<br>• Correio eletrônico (e-mail).<br>• Fax.<br>• Telefone.<br>• TV.<br>• Rádio. |
| Descarte | Ocorre quando a informação não é mais útil e é eliminada ou indiretamente quando o meio que a suportava for substituído.<br>Exemplos:<br>• Descartar na lixeira material impresso.<br>• Descartar na lixeira rascunhos de minutas de relatórios e correspondências.<br>• Substituir um HD por obsolescência.<br>• Troca de um PC.<br>• Destruição de documento por imposição legal. |

## 1.10. O ESTUDO

Nos próximos capítulos passaremos a fazer o estudo do ambiente do Senado Federal, propor estruturas organizacionais para gerir a Segurança da Informação no Senado Federal, um Plano de Implementação da Política de Segurança e uma adaptação da Norma NBR/ISO 17799:2005 como a minuta de uma Nova Política de Segurança da Informação .

Neste estudo adotamos a seguinte metodologia:

A. Estudo das normas vigentes;

B. Entrevista com técnicos de TI da Secretaria Especial de Informática do Senado Federal – Prodasen.

Neste documento não iremos tecer comentários às Políticas de Segurança existentes tendo em vista que o presente documento será público e esta discussão poria em risco a organização. Contudo, as Políticas existentes foram consideradas como subsídio para este trabalho.

# 2. ANÁLISE DO AMBIENTE DO SENADO FEDERAL

Neste estudo nos debruçamos sob dois aspectos do ambiente do Senado Federal:

A. A estrutura organizacional; com vistas a propor áreas para a gestão da Segurança da Informação.

B. As particularidades que o distinguem das demais organizações, para que possamos sugerir uma Nova Política de Segurança da Informação.

## 2.1. ORGANOGRAMA ATUAL DO SENADO FEDERAL

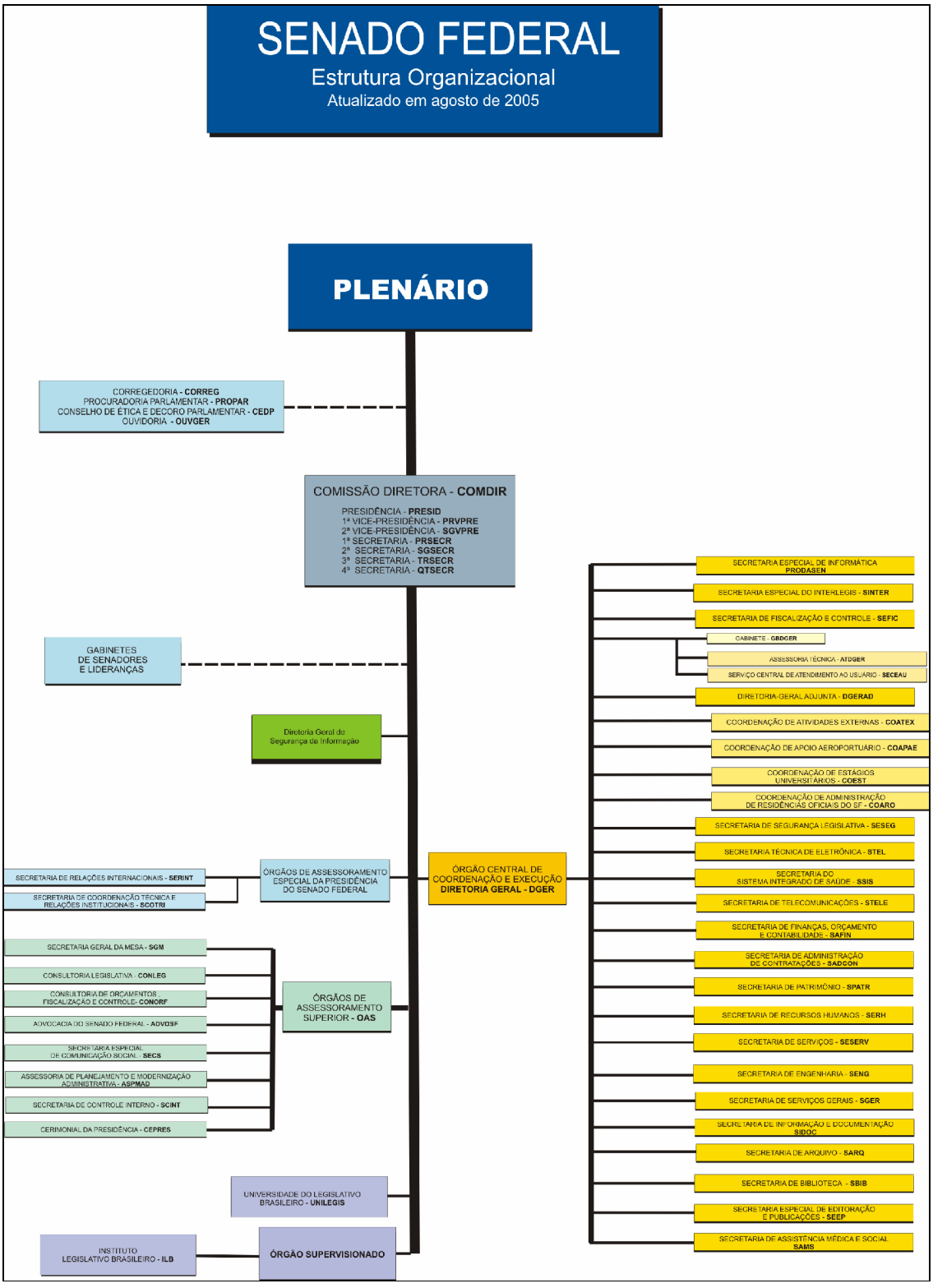



**Figura 2.1 - Organograma do Senado Federal – Resumido.**

## 2.2. PARTICULARIDADES DO SENADO FEDERAL

Tendo em vista a peculiaridade do Senado Federal algumas premissas devem ser consideradas para o planejamento de sua Política de Segurança. Neste trabalho, elencamos as características que julgamos mais importantes. Recomendamos que este tópico seja revisto em profundidade pela Diretoria e Comissões de Segurança que proporemos neste trabalho.

### 2.2.1. O Senado Federal exerce solidariamente com a Câmara dos Deputados um dos poderes da União.

A Constituição da República Federativa do Brasil de 1988 em seus artigos 1º, 2º e 44º caracteriza a Instituição Senado Federal como parte integrante do Poder Legislativo e, por conseguinte, como co-responsável pela manutenção de um dos poderes da União.

> *"Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado democrático de direito e tem como fundamentos:*
> *I - a soberania;*
> *II - a cidadania;*
> *III - a dignidade da pessoa humana;*
> *IV - os valores sociais do trabalho e da livre iniciativa;*
> *V - o pluralismo político.*
> *Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição."*
>
> *"Art. 2º São poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário."*
>
> *Art. 44. O Poder Legislativo é exercido pelo Congresso Nacional, que se compõe da Câmara dos Deputados e do Senado Federal.*

Como parte importante da mais alta estrutura administrativa do país, o Senado deve considerar em sua Política de Segurança a importância da instituição para a administração do Brasil.

### 2.2.2. Objetivo constitucional do Senado.

A Constituição da República Federativa do Brasil de 1988 em seu artigo 3º define o objetivo da República e por conseguinte a missão constitucional do Senado que exerce um dos Poderes da União:

> *"Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:*
> *I - construir uma sociedade livre, justa e solidária;*
> *II - garantir o desenvolvimento nacional;*
> *III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais;*
> *IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação."*

Isto posto, a falha da política de Segurança do Senado Federal poderá comprometer os objetivos constitucionais da República com graves danos para o país.

### 2.2.3. Atividades constitucionais do Congresso e do Senado.

Na mesma linha de raciocínio do item anterior, falhas nas atividades de Segurança da Informação e conseqüentes falhas na atuação do Senado poderão trazer resultados prejudiciais às relações internacionais do Brasil, à vida administrativa do país e ao cotidiano do povo brasileiro, dadas as atribuições do Congresso e do Senado conforme a constituição em seus artigos 4º, 48, 49, 50, 52 e 59:

> *"Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios:*
> *I - independência nacional;*
> *II - prevalência dos direitos humanos;*
> *III - autodeterminação dos povos;*
> *IV - não-intervenção;*
> *V - igualdade entre os Estados;*
> *VI - defesa da paz;*
> *VII - solução pacífica dos conflitos;*
> *VIII - repúdio ao terrorismo e ao racismo;*
> *IX - cooperação entre os povos para o progresso da humanidade;*
> *X - concessão de asilo político.*
> *Parágrafo único. A República Federativa do Brasil buscará a integração econômica, política, social e cultural dos povos da*

*América Latina, visando à formação de uma comunidade latino-americana de nações."*

*Art. 48. Cabe ao Congresso Nacional, com a sanção do Presidente da República, não exigida esta para o especificado nos arts. 49, 51 e 52, dispor sobre todas as matérias de competência da União, especialmente sobre:*
*I - sistema tributário, arrecadação e distribuição de rendas;*
*II - plano plurianual, diretrizes orçamentárias, orçamento anual, operações de crédito, dívida pública e emissões de curso forçado;*
*III - fixação e modificação do efetivo das Forças Armadas;*
*IV - planos e programas nacionais, regionais e setoriais de desenvolvimento;*
*V - limites do território nacional, espaço aéreo e marítimo e bens do domínio da União;*
*VI - incorporação, subdivisão ou desmembramento de áreas de Territórios ou Estados, ouvidas as respectivas Assembléias Legislativas;*
*VII - transferência temporária da sede do Governo Federal;*
*VIII - concessão de anistia;*
*IX - organização administrativa, judiciária, do Ministério Público e da Defensoria Pública da União e dos Territórios e organização judiciária, do Ministério Público e da Defensoria Pública do Distrito Federal;*
*X - criação, transformação e extinção de cargos, empregos e funções públicas, observado o que estabelece o art. 84, VI, b;*
*XI - criação e extinção de Ministérios e órgãos da administração pública;*
*XII - telecomunicações e radiodifusão;*
*XIII - matéria financeira, cambial e monetária, instituições financeiras e suas operações;*
*XIV - moeda, seus limites de emissão, e montante da dívida mobiliária federal;*
*XV - fixação do subsídio dos Ministros do Supremo Tribunal Federal, observado o que dispõem os arts. 39, § 4º; 150, II; 153, III; e 153, § 2º, I.*

*Art. 49. É da competência exclusiva do Congresso Nacional:*

*I - resolver definitivamente sobre tratados, acordos ou atos internacionais que acarretem encargos ou compromissos gravosos ao patrimônio nacional;*

*II - autorizar o Presidente da República a declarar guerra, a celebrar a paz, a permitir que forças estrangeiras transitem pelo território nacional ou nele permaneçam temporariamente, ressalvados os casos previstos em lei complementar;*

*III - autorizar o Presidente e o Vice-Presidente da República a se ausentarem do País, quando a ausência exceder a quinze dias;*

*IV - aprovar o estado de defesa e a intervenção federal, autorizar o estado de sítio, ou suspender qualquer uma dessas medidas;*

*V - sustar os atos normativos do Poder Executivo que exorbitem do poder regulamentar ou dos limites de delegação legislativa;*

*VI - mudar temporariamente sua sede;*

*VII - fixar idêntico subsídio para os Deputados Federais e os Senadores, observado o que dispõem os arts. 37, XI, 39, § 4º, 150, II, 153, III, e 153, § 2º, I;*

*VIII - fixar os subsídios do Presidente e do Vice-Presidente da República e dos Ministros de Estado, observado o que dispõem os arts. 37, XI, 39, § 4º, 150, II, 153, III, e 153, § 2º, I;*

*IX - julgar anualmente as contas prestadas pelo Presidente da República e apreciar os relatórios sobre a execução dos planos de governo;*

*X - fiscalizar e controlar, diretamente, ou por qualquer de suas Casas, os atos do Poder Executivo, incluídos os da administração indireta;*

*XI - zelar pela preservação de sua competência legislativa em face da atribuição normativa dos outros Poderes;*

*XII - apreciar os atos de concessão e renovação de concessão de emissoras de rádio e televisão;*

*XIII - escolher dois terços dos membros do Tribunal de Contas da União;*

*XIV - aprovar iniciativas do Poder Executivo referentes a atividades nucleares;*

*XV - autorizar referendo e convocar plebiscito;*
*XVI - autorizar, em terras indígenas, a exploração e o aproveitamento de recursos hídricos e a pesquisa e lavra de riquezas minerais;*
*XVII - aprovar, previamente, a alienação ou concessão de terras públicas com área superior a dois mil e quinhentos hectares."*

*"Art. 50. A Câmara dos Deputados e o Senado Federal, ou qualquer de suas comissões, poderão convocar Ministro de Estado ou quaisquer titulares de órgãos diretamente subordinados à Presidência da República para prestarem, pessoalmente, informações sobre assunto previamente determinado, importando em crime de responsabilidade a ausência sem justificação adequada.*
*§ 1º Os Ministros de Estado poderão comparecer ao Senado Federal, à Câmara dos Deputados ou a qualquer de suas comissões, por sua iniciativa e mediante entendimentos com a Mesa respectiva, para expor assunto de relevância de seu Ministério.*
*§ 2º As Mesas da Câmara dos Deputados e do Senado Federal poderão encaminhar pedidos escritos de informação a Ministros de Estado ou a qualquer das pessoas referidas no caput deste artigo, importando em crime de responsabilidade a recusa, ou o não-atendimento, no prazo de trinta dias, bem como a prestação de informações falsas."*

*"Art. 52. Compete privativamente ao Senado Federal:*
*I - processar e julgar o Presidente e o Vice-Presidente da República nos crimes de responsabilidade, bem como os Ministros de Estado e os Comandantes da Marinha, do Exército e da Aeronáutica nos crimes da mesma natureza conexos com aqueles;*
*II - processar e julgar os Ministros do Supremo Tribunal Federal, os membros do Conselho Nacional de Justiça e do Conselho Nacional do Ministério Público, o Procurador-Geral da República e o Advogado-Geral da União nos crimes de responsabilidade;*

*III - aprovar previamente, por voto secreto, após argüição pública, a escolha de:*
*a) magistrados, nos casos estabelecidos nesta Constituição;*
*b) Ministros do Tribunal de Contas da União indicados pelo Presidente da República;*
*c) Governador de Território;*
*d) presidente e diretores do Banco Central;*
*e) Procurador-Geral da República;*
*f) titulares de outros cargos que a lei determinar;*
*IV - aprovar previamente, por voto secreto, após argüição em sessão secreta, a escolha dos chefes de missão diplomática de caráter permanente;*
*V - autorizar operações externas de natureza financeira, de interesse da União, dos Estados, do Distrito Federal, dos Territórios e dos Municípios;*
*VI - fixar, por proposta do Presidente da República, limites globais para o montante da dívida consolidada da União, dos Estados, do Distrito Federal e dos Municípios;*
*VII - dispor sobre limites globais e condições para as operações de crédito externo e interno da União, dos Estados, do Distrito Federal e dos Municípios, de suas autarquias e demais entidades controladas pelo poder público federal;*
*VIII - dispor sobre limites e condições para a concessão de garantia da União em operações de crédito externo e interno;*
*IX - estabelecer limites globais e condições para o montante da dívida mobiliária dos Estados, do Distrito Federal e dos Municípios;*
*X - suspender a execução, no todo ou em parte, de lei declarada inconstitucional por decisão definitiva do Supremo Tribunal Federal;*
*XI - aprovar, por maioria absoluta e por voto secreto, a exoneração, de ofício, do Procurador-Geral da República antes do término de seu mandato;*
*XII - elaborar seu regimento interno;*
*XIII - dispor sobre sua organização, funcionamento, polícia, criação, transformação ou extinção dos cargos, empregos e funções de seus serviços, e a iniciativa de lei para fixação da respectiva*

*remuneração, observados os parâmetros estabelecidos na lei de diretrizes orçamentárias;*
*XIV - eleger membros do Conselho da República, nos termos do art. 89, VII.*
*XV - avaliar periodicamente a funcionalidade do Sistema Tributário Nacional, em sua estrutura e seus componentes, e o desempenho das administrações tributárias da União, dos Estados e do Distrito Federal e dos Municípios.*
*Parágrafo único. Nos casos previstos nos incisos I e II, funcionará como Presidente o do Supremo Tribunal Federal, limitando-se a condenação, que somente será proferida por dois terços dos votos do Senado Federal, à perda do cargo, com inabilitação, por oito anos, para o exercício de função pública, sem prejuízo das demais sanções judiciais cabíveis.*

*"Art. 59. O processo legislativo compreende a elaboração de:*
*I - emendas à Constituição;*
*II - leis complementares;*
*III - leis ordinárias;*
*IV - leis delegadas;*
*V - medidas provisórias;*
*VI - decretos legislativos;*
*VII - resoluções.*
*Parágrafo único. Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis*."

### 2.2.4. Atribuição fiscalizadora do Congresso Nacional

Destacamos, em separado, a atribuição do Congresso Nacional na fiscalização das atividades nas quais os Poderes da União ou seus agentes estejam envolvidos. Esta atribuição é dada pelos artigos 58 e 70 da Constituição.

*"Art. 58. O Congresso Nacional e suas Casas terão comissões permanentes e temporárias, constituídas na forma e com as atribuições previstas no respectivo regimento ou no ato de que resultar sua criação.*
*.....*
*§ 2º Às comissões, em razão da matéria de sua competência, cabe:*
*.....*

*II - realizar audiências públicas com entidades da sociedade civil;*
*III - convocar Ministros de Estado para prestar informações sobre assuntos inerentes a suas atribuições;*
*IV - receber petições, reclamações, representações ou queixas de qualquer pessoa contra atos ou omissões das autoridades ou entidades públicas;*
*V - solicitar depoimento de qualquer autoridade ou cidadão;*
*VI - apreciar programas de obras, planos nacionais, regionais e setoriais de desenvolvimento e sobre eles emitir parecer.*
*§ 3º As comissões parlamentares de inquérito, que terão poderes de investigação próprios das autoridades judiciais, além de outros previstos nos regimentos das respectivas Casas, serão criadas pela Câmara dos Deputados e pelo Senado Federal, em conjunto ou separadamente, mediante requerimento de um terço de seus membros, para a apuração de fato determinado e por prazo certo, sendo suas conclusões, se for o caso, encaminhadas ao Ministério Público, para que promova a responsabilidade civil ou criminal dos infratores.*
*.....”*

*“Art. 70. A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder.*
*Parágrafo único. Prestará contas qualquer pessoa física ou jurídica, pública ou privada, que utilize, arrecade, guarde, gerencie ou administre dinheiros, bens e valores públicos ou pelos quais a União responda, ou que, em nome desta, assuma obrigações de natureza pecuniária.”*

A falha na execução desta atividade poderá trazer graves prejuízos ao país e à instituição uma vez que inerentemente requer alto grau de sigilo no tratamento das informações. Algumas informações tratadas nesta atividade só podem ser de conhecimento

público ao final do processo; outras, por outro lado, devem ser mantidas em sigilo indefinidamente mesmo após findo o processo investigatório; e outras, ainda, devem ter seu sigilo mantido por período determinado – tudo de acordo com a Legislação vigente. Além disto, o processo investigatório deve ser claro e transparente, uma vez que o poder Legislativo atua em nome do povo. Portanto, a Política de Segurança deve prever mecanismos para tratar também destas situações.

### 2.2.5. Independência do Senado Federal e dos Poderes da União.

> *"Art. 2º São poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário."*
>
> *"Art. 52. Compete privativamente ao Senado Federal:*
> .....
> *XII - elaborar seu regimento interno;*
> ....."

Sendo os Poderes da União independentes entre si e cabendo, privativamente, ao Senado a elaboração de seu regimento interno, normativas estabelecidas no âmbito dos demais poderes ou na Câmara dos Deputados não tem efeito no âmbito desta instituição. Porém, na elaboração da Política de Segurança da Informação do Senado Federal, as normas adotadas nos demais poderes e Câmara dos Deputados devem ser consideradas, visando obter o melhor resultado possível dados os relacionamentos existentes entre os demais poderes e com a Câmara dos Deputados.

### 2.2.6. O Princípio da Publicidade

Ensina o Prof. Hely Lopes Meirelles [3]: "Em princípio, todo ato administrativo deve ser publicado, porque pública é a Administração que o realiza, só se admitindo sigilo nos casos de segurança nacional, investigações policiais ou interesse superior da Administração a ser preservado em processo previamente declarado sigiloso". Ressaltamos neste ponto também o prescrito no Art. 5º da Constituição Federal:

> *"Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*

> .....
> *XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;*
> .....
> *LXXII - conceder-se-á habeas data:*
> *a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;*
> *b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;*
> .....”

Assim, todo o processo Administrativo do Senado Federal, para que tenha validade, deve ser publicado, muito embora o conteúdo, quando sigiloso, não possa ser revelado. Afinal, sendo a legitimidade do Poder Legislativo respaldada pela vontade popular, ressalvados os casos citados por Hely Lopes Meirelles, não são republicanas as ações que não sejam públicas. Esta preocupação também deve ser levada em consideração na elaboração da Política da Segurança da Informação.

### 2.2.7. Princípios a que estão sujeitos a administração pública

> *“Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:*
> .....”

Estando sujeita aos princípios definidos no artigo 37 da Constituição Federal, que são legalidade, impessoalidade, moralidade, publicidade e eficiência, a Política da Segurança do Senado Federal deverá segui-las, mantendo, porém, o equilíbrio entre os princípios da publicidade e eficiência, uma vez que uma Política de Segurança totalmente pública será ineficiente, pois dará às pessoas mal intencionadas conhecimento sobre eventuais falhas.

### 2.2.8. Estrutura Hierárquica Administrativa do Senado Federal

A mais alta posição no Senado Federal, diferentemente das empresas privadas e órgão do Executivo, é composta pelo colégio de Senadores, o Plenário, cuja vontade (50% dos

Senadores +1) é que determina os rumos da administração da casa. Embora a casa possua uma Mesa Diretora com Presidente, Vices-Presidentes e Secretários, esta Mesa Diretora se subordina à vontade do Plenário. Ressalta-se ainda que a Corregedoria também não se subordina à Mesa Diretora e sim ao Colégio de Senadores, pois não é dado ao Presidente do Senado ou à Mesa poder para julgar os Senadores nem a eles impingir qualquer norma. Toda norma a que os Senadores estarão sujeitos só podem se originar das atividades do Plenário, e e toma forma legal com a votação. Por este motivo, a Política de Segurança da Informação, depois de elaborada, havendo necessidade de se normatizar ação de Senador, deverá ser submetida à apreciação daquele colégio. Cabe ressaltar ainda que, sendo atividade relativa ao Congresso Nacional, Senado Federal e Câmara dos Deputados, a proposta de norma deverá ser avaliada pelo Congresso Nacional (50% dos parlamentares + 1) e, sendo aprovada, tornar-se-á Ato do Congresso Nacional.

A atividade fim do Senado Federal e do Congresso Nacional, que é legislar, é executada exclusivamente pelos Parlamentares. A atividade meio é executada por parlamentares, quando exercendo funções da administração, por servidores públicos e por colaboradores diversos. A atividade meio visa assegurar que a atividade legislativa transcorra com o maior desembaraço possível. Sendo complexa a atividade atribuída ao Senado Federal e ao Congresso Nacional, a atividade meio é realizada por uma organização cuja complexidade podemos depreender da estrutura organizacional. Veja o Organograma do Senado Federal do capítulo 2.1.

Complicando a gestão da casa e, por conseguinte, a elaboração da Política de Segurança do Senado Federal, aos funcionários públicos é aplicada a legislação pertinente à Administração Pública, enquanto que os parlamentares estão sujeitos a normas diferentes, cuja manutenção é de responsabilidade desse próprio corpo de legisladores. Cabe ressaltar, porém, que todos, excetuando-se os casos de colaboradores terceirizados, estão sujeitos ao Regimento Interno do Senado Federal e ao Regimento Comum do Congresso Nacional.

Assim, a Política de Segurança da Informação do Senado Federal, deverá contemplar os diferentes aspectos legais a que estão sujeitos cada grupo de pessoas envolvidas.

### 2.2.9. Servidores e Colaboradores

Quanto às pessoas que trabalham localmente no Senado Federal temos seguinte quadro:

- Senadores.
- Servidores públicos admitidos por concurso público.
- Servidores públicos nomeados em cargos de comissão – (livre nomeação).
- Servidores públicos requisitados – pessoal de outros órgãos do governo que prestam serviços ao Senado Federal.
- Terceirizados – Colaboradores de empresas contratadas para exercerem atividades específicas.
- Estagiários.
- Assessores parlamentares – Funcionários de outros órgãos prestando assessoria aos órgãos de origem pelo acompanhamento da atividade legislativa.

Estas pessoas trabalham no ambiente do Senado Federal e, de modo geral, possuem acesso à rede de computadores do Senado, sendo esta uma das preocupações da Política de Segurança.

### 2.2.10. Acessos externos à rede de computadores do Senado Federal

Além dos acessos realizados localmente à rede de computadores do Senado Federal temos os seguintes acessos externos:

- Acesso a partir das residências oficiais dos Senadores em Brasília mediante ponto de rede instalado naquele local. É considerado Intranet.
- Acesso do escritório regional dos Senadores por meio de VPN. É considerado Intranet.
- Acesso ao portal do Senado pela Web. Temos Internet e Intranet por meio de acesso controlado.

- Transferências de arquivos entre órgãos com os quais Senado mantém convênio. FTP, etc.

Sendo os acessos pontos vulneráveis, a política de Segurança deverá prever os tipos de acessos possíveis e medidas de controle.

### 2.2.11. Acesso físico ao ambiente do Senado Federal

O acesso ao Senado Federal é facultado a toda pessoa, mediante identificação, sendo vetado o acesso ao Plenário (franqueada a galeria), às reuniões secretas das comissões e alguns ambientes de acesso exclusivo aos funcionários autorizados. Dentre o público que freqüenta o ambiente do Senado destaca-se um grande volume de jornalistas, políticos de todas as esferas da administração pública bem como seus colaboradores sejam eles brasileiros ou estrangeiros.

É importante que a Política de Segurança dê suporte a mecanismos de registro e acompanhamento das pessoas que circulam diariamente pelo ambiente do Senado Federal.

Cabe ressaltar ainda que devido à extrema proximidade entre Câmara dos Deputados e Senado Federal, cuja distinção chega a ser imperceptível aos menos atentos, é importante que o controle de acesso seja feito em conjunto com aquela casa para que se torne efetivo. Pois, assim como a informação, pessoas e bens circulam quase que livremente entre as instalações de uma e outra organização.

### 2.2.12. O Processo Legislativo.

> *"Art. 59. O processo legislativo compreende a elaboração de:*
> *I - emendas à Constituição;*
> *II - leis complementares;*
> *III - leis ordinárias;*
> *IV - leis delegadas;*
> *V - medidas provisórias;*
> *VI - decretos legislativos;*
> *VII - resoluções.*
> *Parágrafo único. Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis.*"

Uma característica relevante do processo legislativo é que o mesmo possui duas fases distintas. A primeira, que não é regulamentada, é a fase da "criação" da proposta de

legislação. Esta etapa ocorre dentro da esfera de controle do parlamentar interessado na matéria. A segunda fase do processo, que é regulamentada, diz respeito à tramitação da proposta pelos caminhos do processo Legislativo. Ocorre, porém, que na primeira fase, sendo ainda uma "possibilidade" de proposta, muitas vezes, usa-se a infra-estrutura do Senado para armazenar as minutas e estudos relativos à mesma. Neste momento, os parlamentares possuem uma grande preocupação quanto ao sigilo das informações relativas ao trabalho em andamento, que poderá render-lhe bônus se bem sucedido. Se, neste momento, outro parlamentar vier a apresentar a mesma idéia, poderá surgir a suspeita de espionagem ou mau trabalho dos funcionários da casa. Cabe ressaltar, porém, que após apresentada a proposta de norma, já na segunda fase, os parlamentares, de modo geral, têm interesse que o trabalho seja de amplo conhecimento público. Verificamos assim, existirem dois momentos distintos na elaboração de uma proposta de legislação que a Política de Segurança do Senado deve tratar.

### 2.2.13. Atividades do Congresso Nacional

> *Art. 44. O Poder Legislativo é exercido pelo Congresso Nacional, que se compõe da Câmara dos Deputados e do Senado Federal.*

Outro ponto que a Política de Segurança da Informação do Senado terá de tratar são as questões advindas da natureza do Poder Legislativo que é exercido efetivamente pelo Congresso Nacional, Senado Federal e Câmara dos Deputados. Desta natureza decorre que existem atividades que são realizadas pelo conjunto das duas casas, compartilhando informações ou recursos. Os processos legislativos ocorrem em atividades seqüenciais separadas e também em processos cujas atividades são unificadas, tais como as das comissões mistas. Para regular as atividades que são seqüenciais e separadas existem regimentos internos para cada uma das casas, e ainda, uma norma específica para quando as atividades são conjuntas, o Regimento Comum. Por este motivo, a Política de Segurança deve considerar meios para que a troca de informações e recursos seja segura em todas as etapas do processo legislativo, quaisquer que sejam eles.

### 2.2.14. Sistemas fora da rede do Senado Federal

Devido à importância de alguns sistemas, tal como o Sistema de Votação, eles são isolados da rede e sua manutenção é realizada por equipe especial. Esta necessidade especial também deve estar definida na Política de Segurança do Senado Federal.

### 2.2.15. Retorno sobre o investimento

Alguns autores sugerem que devido à impossibilidade de alocar recursos para proteger todos os ativos da organização deve-se avaliar o risco de cada item em relação ao ROI – *Return Of Investment* – Retorno sobre o investimento. No caso do Senado Federal isto não poderá ser feito de maneira clássica uma vez que o orçamento da casa é elaborado por ela mesma e faz parte do Orçamento Geral da União, que é estabelecido pelo Congresso e sancionado pelo Poder Executivo. Grosso modo, para o orçamento da casa não há limitação, pois o que se produz – legislação, fiscalização das atividades da União, etc. – visa ao Bem Comum do país e não poderia sofrer restrições. Porém, uma forma de medir se o investimento em determinado item de segurança seria adequado é avaliá-lo quanto ao retorno esperado pela sociedade das atividades realizadas do Senado Federal. Isto é, se o item de segurança irá melhorar a imagem da instituição, a confiança que a sociedade tem nela, e ainda, se os processos legislativos produzem estabilidade institucional medidos pela segurança que os processos exigem e não pelas ações políticas. Esta abordagem parece ser a mais adequada uma vez que é a sociedade que, através dos impostos, fornece recursos para o Orçamento da União e conseqüentemente para o orçamento da casa.

# 3. LEGISLAÇÃO EXISTENTE

Apresentamos neste capítulo a legislação existente, não esgotando, porém, o levantamento, uma vez que a legislação brasileira é vasta e existem normas internacionais que não foram aqui consideradas, mas que, no futuro, poderão ser utilizadas para subsidiar a atualização da Política de Segurança da Informação, que não deve estar congelada no tempo, mas sim constantemente atualizada e aperfeiçoada em virtude de mudanças organizacionais, ambientais, humanas e tecnológicas.

## 3.1. A LEGISLAÇÃO

**Tabela 3.1 - Legislação.**

| **Tipo** | **Descrição** | |
|---|---|---|
| CF | Constituição Federal | |
| Medida Provisória | 2.200-2, de 24 de agosto de 2001. | Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituo Nacional de Tecnologia da Informação em autarquia, e dá outras providências. |
| Leis | 6.538, de 22 de junho de 1978. | Dispõe sobre os Serviços Postais. |
| | 7.170, de 14 de dezembro de 1983. | Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. |
| | 8.027, de 12 de abril de 1990. | Dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências. |

| Tipo | Descrição | |
|---|---|---|
| Leis | 8.112, de 11 de dezembro de 1990. | Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. |
| | 8.159, de 8 de janeiro de 1991. | Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. |
| | 8.429, de 2 de junho de 1992. | Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. |
| | 8.666, de 21 de junho de 1993. | Institui normas para licitações e contratos da Administração Pública e dá outras providências. |
| | 9.279, de 14 de maio de 1996. | Regula direitos e obrigações relativos à propriedade industrial. |
| | 9.983, de 14 de julho de 2000. | Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. |
| | 10.520, de 17 de julho de 2002. | Institui, no âmbito da União, estados, Distrito Federal e municípios, nos termos do artigo 37, inciso xxi, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências. |

| Tipo | Descrição | |
|---|---|---|
| Leis | 11.111, de 5 de maio de 2005. | Regulamenta a parte final do disposto no inciso XXXIII do caput do art. 5º da Constituição Federal e dá outras providências. |
| Lei GDF (1) | 2.572, de 20 de julho de 2000. | Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática. |
| Decretos (2) | 1.171, de 22 de junho de 1994. | Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal. |
| | 1.173, de 2 de junho de 1994. | Dispõe sobre a competência, organização e funcionamento do Conselho Nacional de Arquivos (CONARQ) e do Sistema Nacional de Arquivos (SINAR) e dá outras providências. |
| | 3.505, de 13 de junho de 2000. | Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. |
| | 3.587, de 5 de setembro de 2000. | Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov, e dá outras providências. |
| | 3.996, de 31 de outubro de 2001. | Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. |

| Tipo | Descrição | |
|---|---|---|
| Decretos (2) | 4.073, de 3 de janeiro de 2002. | Regulamenta a Lei no 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. |
| | 4.273, de 20 de junho de 2002. | Dispõe sobre a cessão de servidores de órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional. |
| | 4.497, de 4 de dezembro de 2002. | Dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles, e dá outras providências. |
| | 4.553, de 27 de dezembro de 2002. | Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. |
| | 4.915, de 12 de dezembro de 2003. | Dispõe sobre o Sistema de Gestão de Documentos de Arquivo - SIGA, da administração pública federal, e dá outras providências. |
| | 5.301, de 9 DE dezembro de 2004. | Regulamenta o disposto na Medida Provisória nº 228, de 9 de dezembro de 2004, que dispõe sobre a ressalva prevista na parte final do disposto no inciso XXXIII do art. 5o da Constituição, e dá outras providências. |
| Decretos GDF | 25.750, de 12 de abril | Regulamenta a Lei nº 2.572, de 20 de julho de 2000, que “Dispõe sobre a prevenção das |

| Tipo | Descrição | |
|---|---|---|
| (1) | de 2005. | entidades públicas do DF com relação aos procedimentos praticados na área de informática". |
| Resoluções do Congresso Nacional | 1, de 1970 | Regimento Comum do Congresso Nacional. |
| Resoluções do Senado Federal | 93, de 1970 | Regimento Interno do Senado Federal. |
| | 58, de 1972 | Regimento Administrativo do Senado Federal |
| | 11, de 1996 | Regulamenta o credenciamento de profissionais da área de comunicação social, dispõe sobre o Comitê de Imprensa do Senado Federal e dá outras providências. |
| | 9, de 1997 | Altera o Regimento Administrativo do Senado Federal. |
| | 20, de 1993 | Institui o Código de Ética e Decoro Parlamentar. |
| Resoluções do STF (2) | 246, de 2002 | Institui o Código de Ética dos Servidores do Supremo Tribunal Federal e cria a Comissão de Ética. |
| | 247, de 2002 | Regulamenta a aplicação dos institutos de nomeação, designação, posse, exercício, exoneração e dispensa no âmbito do Supremo |

| Tipo | Descrição | |
|---|---|---|
| | | Tribunal Federal e dá outras providências. |
| Atos do Presidente do Congresso Nacional | 109, DE 1997 | Disciplina a venda de avulsos e diários do Senado Federal e do Congresso Nacional; o fornecimento de cópias; e dá outras providências. |
| | 168, de 2003 | Dispõe sobre o acesso e a salvaguarda aos documentos sigilosos do Senado Federal e do Congresso Nacional. |
| Atos do 1º-Secretário | 5, de 1990 | Institui normas para a produção de Impressos Institucionais do Senado Federal. |
| | 2, de 1995 | Regula a entrada de pessoas no Senado Federal. |
| | 6, de 1980 | Regula as áreas de segurança do Senado Federal. |
| | 25, de 2003 | Dispõe sobre o uso e a administração do Serviço de Acesso Remoto da Rede Local do Senado Federal – SARE, baseado na tecnologia VPN (*Virtual Private Network*). |
| | 26, de 2003 | Dispõe sobre o uso e administração do Sistema de Correio Eletrônico do Senado Federal. |
| | 45, de 2004 | Regulamenta a cessão a terceiros de áreas destinadas à realização de eventos culturais |

| Tipo | Descrição | |
|---|---|---|
| | | científicos ou tecnológicos. |
| Atos da Comissão Diretoria do Senado Federal | 17, de 1987 | Regulamenta o credenciamento de representantes de Órgãos Públicos e entidades diversas junto ao Senado Federal. |
| | 09, de 1996 | Dispõe sobre a gestão dos contratos e dá outras providências. |
| | 06, de 1998 | Regulamenta o arquivamento das gravações em áudio do Senado Federal. |
| | 05, de 2000 | Instituí o Sistema de Arquivo e Controle de Documentos do Senado Federal e do Congresso Nacional - SIARQ-SF, integrante do Sistema de Arquivo do Poder Legislativo Federal e do Sistema Nacional de Arquivos - SINAR, de acordo com o item III, Art. 12, do Decreto nº 1.173 de 29-06-94, e do Art. 17, da Lei nº 8.159, de 08-03-91. |
| | 13, de 2005 | Regulamenta no âmbito do Senado Federal e de seu Órgão supervisionado, a Lei nº 8.666, de 21 de junho de 1993 e a Lei, nº 10.520, de 17 de julho de 2002. |
| | 14, de 2005 | Regulamenta a entrada de visitantes no Senado Federal. |

| Tipo | Descrição | |
|---|---|---|
| Atos da Comissão Diretoria do Senado Federal | 16, de 2005 | Regulamenta, no âmbito do Senado Federal e de seu órgão supervisionado, o fornecimento de cópias de documentos. |
| | 18, de 1998 | Regulamenta a Subsecretaria de Segurança Legislativa. |

Observações:

(1) A Legislação do Governo do Distrito Federal foi citada aqui como subsídio para a elaboração de medidas no âmbito do Senado Federal. Essa legislação não tem valor legal na esfera Federal.

(2) Os Atos do Executivo e do Judiciário não têm efeito direto no poder Legislativo, porém a legislação desses poderes deve ser utilizada como referência para a elaboração de medidas no âmbito do Senado Federal.

# 4. PROPOSTA DE UMA NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA O SENADO FEDERAL

Seguindo recomendações da Norma ABNT NBR ISO/IEC 17799:2005, Manual de Boas Práticas em Segurança da Informação [4] do TCU e de especialistas da área de Segurança da Informação propomos a elaboração de uma Nova Política de Segurança da Informação para o Senado Federal seguindo conceitos experimentados em diversas empresas e também preconizados internacionalmente.

Assim proporemos diversas ações para que uma Nova Política de Segurança da Informação do Senado Federal seja elaborada e que a mesma seja eficiente.

## 4.1. DIRETORIA DE SEGURANÇA DA INFORMAÇÃO E DE COMISSÕES SEGURANÇA DA INFORMAÇÃO

Inicialmente propomos de criação da Diretoria de Segurança da Informação e de Comissões de Segurança da Informação. Esta proposta visa criar na estrutura organizacional um órgão com autonomia para implantar a Política de Segurança da Informação e garantir a sua implementação. Este órgão é denominado pelos especialistas de Comitê de Segurança da Informação. Por razões históricas e culturais, no Senado Federal resolvemos denominar esse Comitê de Diretoria.

O Tribunal de Contas da União no item 2.4 de seu manual de “Boas Práticas em Segurança da Informação” preconiza:

> *2.4. Quem são os responsáveis por elaborar a PSI?*
>
> *É recomendável que na estrutura da organização exista uma área responsável pela segurança de informações, a qual deve iniciar o processo de elaboração da política de segurança de informações, bem como coordenar sua implantação, aprová-la e revisá-la, além de designar funções de segurança.*
>
> *Vale salientar, entretanto, que pessoas de áreas críticas da organização devem participar do processo de elaboração da PSI, como a alta administração e os diversos gerentes e proprietários dos sistemas informatizados. Além*

> *disso, é recomendável que a PSI seja aprovada pelo mais alto dirigente da organização.*

A norma ABNT NBR ISO/IEC 17799:2005 recomenda o seguinte no item 6.1.2:

> *6.1.2 Coordenação da segurança da informação*
>
> *Controle*
>
> *Convém que as atividades de segurança da informação sejam coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.*
>
> *Diretrizes para implementação*
>
> *Convém que a coordenação da segurança da informação envolva a cooperação e colaboração de gerentes, usuários, administradores, desenvolvedores, auditores, pessoa da segurança e especialistas com habilidades nas áreas de seguro, questões legais, recursos humanos, TI e gestão de riscos.*

Marcos Sêmola em seu livro Gestão da Segurança da Informação no item 4.5 escreve o seguinte:

> *4.5 Comitê Corporativo de Segurança da Informação*
>
> *Representando o núcleo concentrador dos trabalhos, o Comitê Corporativo de Segurança da Informação deve estar, além de adequadamente posicionado no organograma, formado a partir da clara definição de seu objetivo, estrutura, funções responsabilidades, perfil dos executores, além da formal e oficial identificação de seus membros, que darão representatividade aos departamentos mais críticos e relevantes da empresa.*
>
> *Reunir gestores com visões do mesmo objeto, mas de pontos distintos, é fundamental para a obtenção da nítida imagem dos problemas, desafios e impactos. Por isso deve envolver representantes das áreas Tecnológica, Comunicação, Comercial, Negócios, Jurídico, Patrimonial, Financeira, Auditoria, etc., em muito agregará para o processo de gestão, de forma a evitar conflitos, desperdícios, redundâncias e o principal: fomentar a sinergia da empresa intimamente alinhada à suas diretrizes estratégicas de curto, médio e longo prazos.*

Isto posto, vale salientar que em algumas organizações ocorre um erro comum de atribuírem à área de TI a responsabilidade pela implementação da PSI – Política de Segurança da Informação e a elaboração do PISI – Plano de Implementação da Segurança da Informação. Desta maneira os resultados desejados não são totalmente alcançados porque, devido à sua posição hierárquica dentro da organização, a área de TI não possui suficiente autoridade para impor a PSI e PISI, fiscalizar a implementação e, eventualmente, aplicar sanções. Reconhecendo este fato a Norma ABNT NBR ISO/IEC 17799:2005 recomenda juntamente com especialistas no assunto recomendam a criação de um grupo de trabalho com essa atribuição que é designado pelos especialistas como COMITÊ CORPORATIVO DE SEGURANÇA DA INFORMAÇÃO. Este comitê, devidamente posicionado na hierarquia, realizará a gestão da segurança informação na organização. Seguindo esta orientação seria um erro designar ao Prodasen a responsabilidade pela gestão da segurança da informação de todo o Senado Federal uma vez que é uma Secretaria a não ser que houvesse um reposicionamento do Prodasen e este passasse a estar subordinado diretamente à Mesa Diretora do Senado Federal. Porém na situação atual cabe ao Prodasen implementar várias ações de segurança bem como subsidiar com informações técnicas as ações de Política de Segurança da Informação. Observando a cultura e complexidade organizacional do Senado Federal bem como suas características peculiares propomos a criação de uma Diretoria Geral de Segurança da Informação, Comissões Permanentes de Segurança da Informação e, nas Secretarias uma Subsecretaria de Segurança da Informação e nos demais órgãos onde não couber uma Subsecretaria uma Assessoria de Segurança da Informação. Estes órgãos irão executar as funções normalmente atribuídas pelos especialistas ao Comitê de Segurança da Informação. De modo geral as atribuições destes órgãos serão as seguintes:

- Caberá à Diretoria Geral de Segurança da Informação aplicar as medidas necessárias e adequadas para assegurar a segurança da Informação no Senado Federal.

- Caberá às Comissões Permanentes de Segurança da Informação fornecer subsídios à Diretoria de Segurança da Informação, propor ações às Diretorias/Assessorias de Segurança da Informação.

- Caberá às Subsecretarias/Assessorias de Segurança da Informação zelar pela segurança da informação na área sob sua responsabilidade aplicando as

determinações da Diretoria Geral de Segurança da Informação e orientações das Comissões Permanentes de Segurança da Informação.

As Comissões serão criadas em número adequado de modo a assegurar a participação de todos os órgãos envolvidos com a segurança da informação e serão constituídas de acordo com as necessidades do Senado Federal. Algumas deverão ser permanentes e outras constituídas para fins específicos. Desta forma recomendamos a da Diretoria Geral de Segurança da Informação, as Diretorias de Segurança da Informação/Assessorias de Segurança da Informação e das Comissões de Segurança da Informação como segue.

### 4.1.1. Posicionamento hierárquico proposto

Conforme proposto na norma ABNT NBR ISO/IEC 17799:2005 no item 6.1.2, bem como pelo manual de Boas Práticas de Segurança da Informação do TCU citados anteriormente recomenda que a área responsável pela segurança de informações seja subordinada a mais alta autoridade. Portanto, no Senado Federal, a Diretoria Geral de Segurança da Informação e das Comissões de Segurança deverão estar subordinadas diretamente à Mesa Diretora do Senado, de modo que possua autoridade suficiente para realizar sua missão. Isto é necessário, pois as determinações dessa Diretoria, aprovadas pela Presidente da Mesa Diretora, deverão ser seguidas por todos os órgãos do Senado Federal.

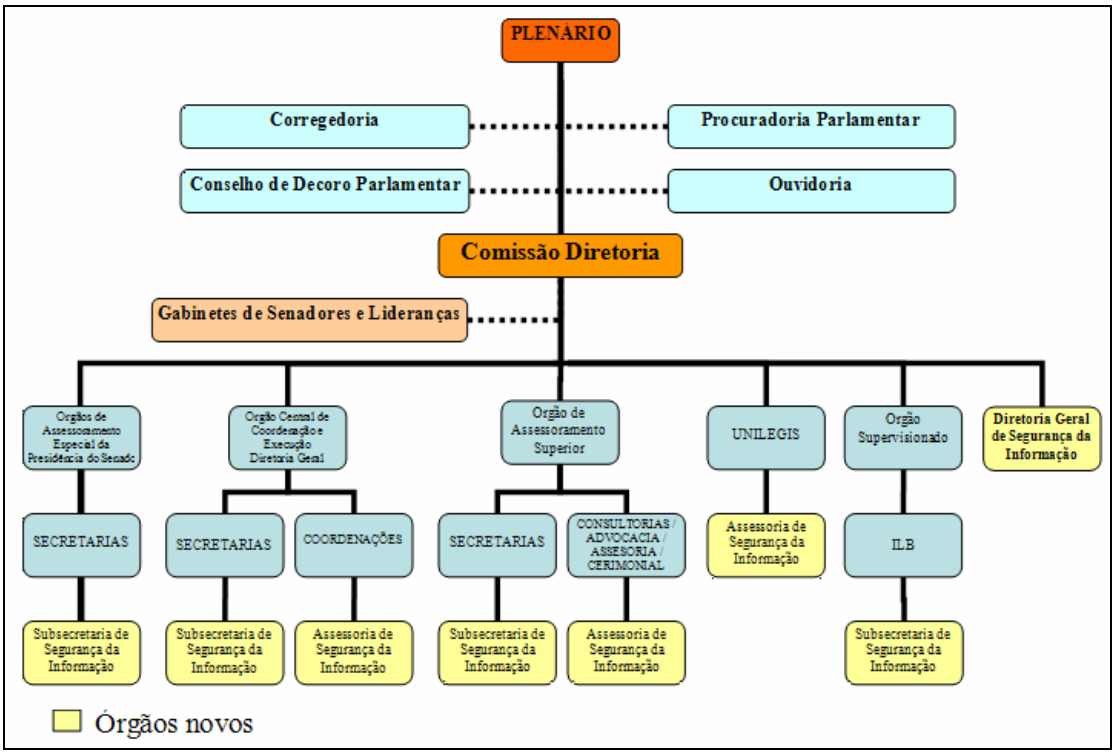



**Figura 4.1 - Organograma Proposto (esquematizado).**

### 4.1.2. Proposta de composição das Comissões de Segurança da Informação

Devido à peculiaridade do Senado Federal e sua complexa estrutura organizacional sugerimos, a principio a criação das seguintes Comissões Permanentes de Segurança.

#### 4.1.2.1. Comissão Permanente de Segurança da Informação – Área Técnica

Constituída por membros das áreas técnicas do Senado Federal que têm à missão implementar ações corporativas de segurança da Informação. Recomendamos tomam parte desta comissão representantes de/da/do:

1. Advocacia do Senado Federal
2. Assessoria de Planejamento e Modernização Administrativa
3. COM. P. DE SEGURANÇA DA INFORMAÇÃO – USUÁRIOS A
4. Comissão Permanente de Segurança da Informação – Usuários B
5. Comissão Permanente de Segurança da Informação – Usuários C

6. Consultoria de Orçamentos Fiscalização e Controle
7. Secretaria de Arquivo
8. Secretaria de Controle Interno
9. Secretaria de Engenharia
10. Secretaria de Finanças, Orçamento e Contabilidade
11. Secretaria de Fiscalização e Controle
12. Secretaria de Informação e Documentação
13. Secretaria de Patrimônio
14. Secretaria de Recursos Humanos
15. Secretaria de Segurança Legislativa
16. Secretaria de Telecomunicações
17. Secretaria de Administração de Contratações
18. Secretaria Especial de Informática - Prodasen
19. Secretaria Técnica de Eletrônica

#### 4.1.2.2. Comissão Permanente de Segurança da Informação – Usuários A

Constituída por membros das áreas usuárias da infra-estrutura de Tecnologia da Informação, Comunicação, Editoração e outros recursos fornecidos pelas áreas técnicas. Recomendamos tomam parte desta comissão representantes de/da/do:

1. Comissão Permanente de Segurança da Informação – Área Técnica
2. Comissão Permanente de Segurança da Informação – Usuários B
3. Comissão Permanente de Segurança da Informação – Usuários C
4. Coordenação de Administração de Residências Oficiais do SF.

5. Coordenação de Apoio Aeroportuário,
6. Coordenação de Atividades Externas,
7. Coordenação de Estágios Universitários,
8. Diretoria Geral
9. Secretaria de Assistência Médica e Social
10. Secretaria de Biblioteca
11. Secretaria de Serviços
12. Secretaria de Serviços Gerais

#### 4.1.2.3. Comissão Permanente de Segurança da Informação – Usuários B

Constituída por membros das áreas usuárias da infra-estrutura de Tecnologia da Informação, Comunicação, Editoração e outros recursos fornecidos pelas áreas técnicas que apresentam características peculiares. Recomendamos que tomem parte desta comissão representantes de/da/do:

1. Cerimonial da Presidência
2. Comissão Permanente de Segurança da Informação – Área Técnica
3. Comissão Permanente de Segurança da Informação – Usuários A
4. Comissão Permanente de Segurança da Informação – Usuários C
5. Consultoria Legislativa
6. Instituto Legislativo Brasileiro – ILB
7. Secretaria de Coordenação Técnica e Relações Institucionais
8. Secretaria de Relações Internacionais
9. Secretaria Especial de Comunicação Social
10. Secretaria Especial de Editoração e Publicações

11. Secretaria Especial do INTERLEGIS
12. Secretaria Geral da Mesa
13. Subsecretaria de Sistema Integrado de Saúde
14. Universidade do Legislativo – UNILEGIS

#### 4.1.2.4. Comissão Permanente de Segurança da Informação – Usuários C

Constituída por representantes dos Gabinetes da/das/dos:

1. Presidência
2. 1ª Vice Presidência
3. 2ª Vice Presidência
4. 1ª Secretaria Geral da Mesa
5. 2ª Secretaria Geral da Mesa
6. 3ª Secretaria Geral da Mesa
7. 4ª Secretaria Geral da Mesa
8. Câmara dos Deputados
9. Comissão Permanente de Segurança da Informação – Usuários A
10. Comissão Permanente de Segurança da Informação – Usuários Área Técnica
11. Comissão Permanente de Segurança da Informação – Usuários B
12. Conselho de Ética e Decoro Parlamentar
13. Corregedoria
14. Gab. Lideranças (1 representante para 14 gabinetes – informação de 01/08/2006)

15. Gab. Senadores – A (1 representante para 16 gabinetes)

16. Gab. Senadores – B (1 representante para 16 gabinetes)

17. Gab. Senadores – C (1 representante para 16 gabinetes)

18. Gab. Senadores – D (1 representante para 16 gabinetes)

19. Gab. Senadores – E (1 representante para 17 gabinetes)

20. Ouvidoria

21. Procuradoria Parlamentar

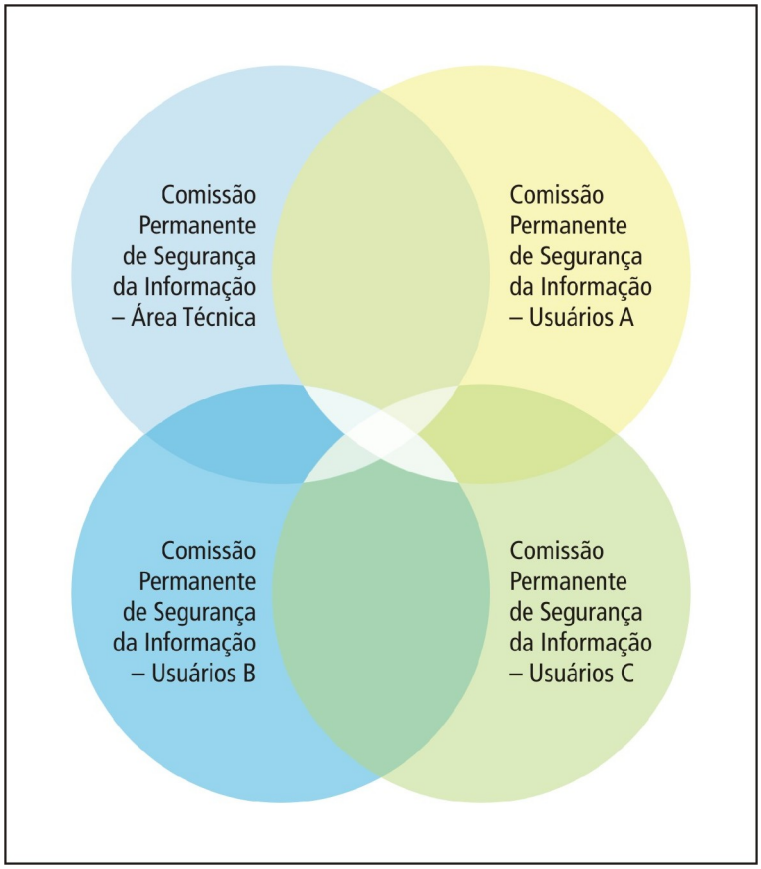



**Figura 4.2 - Comissões de Segurança da Informação.**

#### 4.1.2.5. Subcomissão Permanente de Segurança da Informação – Gab. Senadores

Serão constituídas cinco subcomissões, quatro com 16 representantes e uma com 17, dando a estes oportunidades de participação nas atividades de segurança da Informação. Estas subcomissões são necessárias devido ao grande número de usuários distintos que serão representados e com o objetivo de simplificar a estrutura das comissões.

#### 4.1.2.6. Subcomissão Permanente de Segurança da Informação – Gab. Lideranças

Será constituída uma subcomissão para representar os gabinetes das Lideranças dando a estes oportunidades de participação nas atividades de segurança da Informação.

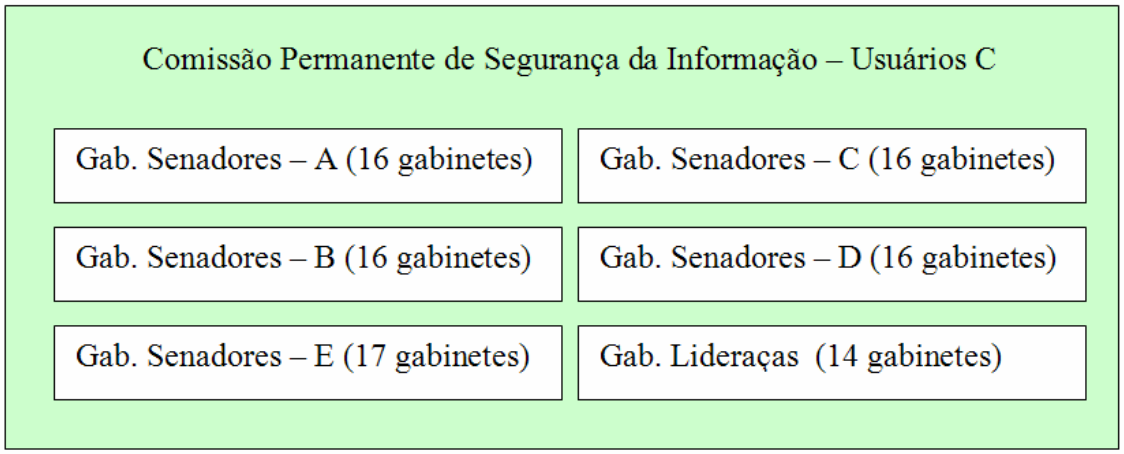



**Figura 4.3 - Subcomissões da Comissão Permanente de Segurança da Informação - Usuários C.**

A Comissão Permanente de Segurança da Informação – Usuários Área Técnica, Comissão Permanente de Segurança da Informação – Usuários A, Comissão Permanente de Segurança da Informação – Usuários B Comissão Permanente de Segurança da Informação – Usuários C deverão nomear um representante para participar da outras. As Subcomissões da Comissão Permanente de Segurança da Informação – Usuários C deverão indicar 1 representante cada para participar da Comissão Permanente de Segurança da Informação – Usuários C.

Justificamos a inclusão de um representante da Câmara dos Deputados na Comissão Permanente de Segurança da Informação – Usuários C para agilizar a implementação de medidas comuns entre as duas casas legislativas devido à proximidade dos ambientes físicos e operacionais bem como pela semelhança das atividades exercidas pelas duas casas e ainda porque ambas compõem o Congresso Nacional. É relevante também que nas atividades do Congresso os procedimentos de segurança devam ser de conhecimento e aplicáveis a todos os envolvidos de quaisquer das casas. Este procedimento permitira que as Políticas de Segurança da Informação de ambas as casas possam ser implementadas em conjunto ou em complementaridade.

#### 4.1.2.7. Cargos propostos para as comissões e subcomissões.

Propomos, de acordo com o costume da casa, que as Comissões e Subcomissões tenham os seguintes cargos:

- Presidente;
- Vice-Presidente;
- Secretário;
- Membros (demais participantes).

### 4.1.3. Atribuições gerais dos membros das comissões.

Cada membro representante deverá ter em seu órgão de origem autoridade para fazer implementar as decisões das Comissões de Segurança da Informação e da Diretoria Geral de Segurança da Informação bem como para expressar as necessidades reais do órgão que representa. Por este motivo recomendamos que os representantes sejam os titulares das Secretarias ou Assessorias propostas neste estudo.

### 4.1.4. Subsecretarias e Assessorias de Segurança da Informação

Tendo em vista a alta complexidade organizacional do Senado Federal cada órgão deverá possuir um Gestor da Segurança da Informação que ficará responsável pela implementação, no seu nível, da PSI e do PISI definidos pela Diretoria Geral de Segurança da Informação e pelas Comissões de Segurança da Informação.

Devido à cultura existente no Senado Federal denominamos os órgãos de Subsecretaria de Segurança da Informação ou Assessoria de Segurança da Informação de acordo com a localização dentro da estrutura hierárquica. Estes deverão estar em contato direto com o Diretor Geral da Segurança da Informação e deve ser o representante das áreas nas Comissões de Segurança da Informação.

Recomendamos ainda, que os gestores citados aqui sejam os titulares das Subsecretarias e Assessorias de Segurança da Informação.

Sugerimos, também, que sendo complexa a atividade de implementação da PSI e do PISI nos níveis mais baixos da organização poderá ser necessário estabelecer Agentes de Segurança nesses níveis também. Caberá aos titulares de cada Subsecretaria/Assessoria avaliar a necessidade e propor a existência deste agente. A criação desta função deverá avaliar a possibilidade de acumulo de funções com outras já existentes.

### 4.1.5. Missão da Diretoria Geral de Segurança da Informação e das Comissões de Segurança da Informação.

Sugerimos que a missão da Diretoria Geral de Segurança seja a seguinte:

**Garantir a segurança da informação no Senado Federal em todo o seu ciclo de vida e em todas as áreas da casa visando proteger a instituição das ameaças que possam prejudicar os processos administrativos ou legislativos do Poder Legislativo Federal.**

### 4.1.6. Atividades da Diretoria Geral de Segurança da Informação

1. Orientar as ações corporativas de Segurança e todas as etapas do PISI - Plano de Implantação da Segurança da Informação.

2. Assegurar o melhor uso dos recursos disponíveis.

3. Coordenar as ações das Subsecretarias/Assessorias de Segurança da Informação com a finalidade manter todos trabalhando com o mesmo objetivo e, se for o caso, determinar os ajustes necessários.

4. Garantir o sucesso do PISI.

5. Promover a consolidação do PISI.

### 4.1.7. Missão das Subsecretarias e Assessorias de Segurança da Informação.

Sugerimos que das Subsecretarias e Assessorias de Segurança da Informação seja a seguinte:

> **Garantir a segurança da informação no seu nível de atuação e em todo o ciclo de vida da informação visando proteger as atividades administrativas e legislativas das ameaças que possam prejudicar o órgão onde atua ou o Poder Legislativo Federal.**

### 4.1.8. Atividades das Subsecretarias/Assessorias de Segurança da Informação

1. Orientar as ações de Segurança e todas as etapas do PISI - Plano de Implementação da Segurança da Informação na sua área de atuação.
2. Assegurar o melhor uso dos recursos disponíveis na sua área de atuação.
3. Implementar as ações de Segurança da Informação de acordo com as Políticas de Segurança da Informação e o PISI.
4. Interagir com as Comissões de Segurança e a Diretoria Geral de Segurança da Informação.

### 4.1.9. Atividades das Comissões de Segurança da Informação

1. Fomentar a implantação do PISI através de ações distribuídas e integradas com abrangência nos aspectos físico, tecnológico e humano interferindo sugerindo melhorias nos processos administrativos e Legislativos para a garantia da Segurança da Informação.
2. Acompanhar os resultados das ações de segurança de forma a medir os efeitos, comparando-os às metas estabelecidas e, quando for o caso, propor

medidas de ajustes necessários no âmbito corporativo e de cada área ou mesmo ajustes nas Políticas de Segurança da Informação.

3. Alinhar as ações das comissões de segurança e das Subsecretarias/Assessorias coletando, com máxima riqueza de detalhes, os fatos relacionados aos aspectos físicos tecnológicos e humanos inerentes à sua esfera de atuação.

## 4.2. PISI – PLANO DE IMPLEMENTAÇÃO DA SEGURANÇA DA INFOMAÇÃO

A primeira etapa para a implantação da Nova Política de Segurança é criar a Diretoria Geral de Segurança da Informação e as Subsecretarias/Assessorias de Segurança da Informação e as Comissões de Segurança da Informação que foi sugerido no item 4.1. Porém, não basta criar a estrutura organizacional e acreditar que tudo ocorrerá bem daí por diante. É necessário adotar um Modelo de Gestão Corporativa de Segurança da Informação, ou seja, um Plano de Implementação da Segurança da Informação que aqui abreviaremos pela sigla PISI. Para este plano sugerimos as seguintes etapas:

### 4.2.1. Mapeamento de Segurança.

*"Não se pode controlar o que não se pode medir" – Lord Kelvin.*

*"Não se pode gerenciar o que não se pode medir" – Tom de Marco.*

O primeiro passo na Implementação da Segurança da Informação consiste em relacionar todos os ativos da instituição e analisar, do ponto de vista da segurança da informação, os prejuízos decorrentes da perda de uma de suas propriedades. Ver item 1.3 deste estudo.

O objetivo é mapear os riscos e vulnerabilidades estabelecendo planos de ação para cada item. Devem-se registrar todos os ativos físicos, tecnológicos e humanos que sustentam os processos da casa, considerando também as variáveis internas e externas que interferem nos riscos/vulnerabilidades e as co-relações entre cada um. Esta atividade deve ser realizada com o auxílio de todos os gestores de ativos e as Comissões de Segurança da

Informação devem estar envolvidas no processo. Damos alguns exemplos de itens a ser mapeado:

**A. No aspecto humano**

Deve ser verificado qual o risco para a instituição se determinada colaborador (senador, funcionário público, terceirizado, etc.), tendo em vista a função e o conhecimento que possui, vir a aposentar-se; vir a falecer repentinamente, for seqüestrado e dele forem exigidas senhas de acesso, verificar o risco de determinado colaborador vir a ser chantageado com o objetivo de oferecer informações relevantes, etc.;

**B. No aspecto físico**

Deve-se verificar qual o impacto decorrente de incêndio, inundação, sabotagem de equipamentos, danos gerados por tumultos, ameaças de bombas, roubo de equipamentos, roubo de *notebooks*, etc.

**C. No aspecto tecnológico**

Devem ser verificados os riscos de falhas de software e hardware, acessos indevidos, impacto de novas tecnologias de armazenamento como os *pen drives*, etc.

O mapeamento consiste em:

4. Inventariar os ativos.
5. Identificar o grau de relevância de cada ativo.
6. Identificar as relações diretas e indiretas entre os diversos processos, perímetro e infra-estrutura.
7. Mapear as necessidades e as relações da organização associadas ao manuseio, armazenamento, transporte e descarte de informações.
8. Priorizar as demandas de segurança.

### 4.2.2. Estabelecer a Estratégia de Segurança.

Consiste em:

1. Definir um plano de ação bianual para o Senado Federal, seguindo a duração do mandato da Mesa Diretora, que considere todas as particularidades estratégias, táticas e operacionais mapeadas na etapa anterior, além dos aspectos de risco físicos, humanos e tecnológicos.

2. Criar sinergia entre os cenários atual e desejado, além da sintonia de expectativas entre os diversos níveis de administração do Senado Federal a fim de obter comprometimento e apoio explicito às medidas previstas no plano de ação.

### 4.2.3. Elaborar o Planejamento da Segurança.

Consiste em:

1. Orientar a organização das Subsecretarias/Assessorias, especificando responsabilidades, posicionamento e escopo de atuação, oficializando seu papel de ações locais em sintonia com ações corporativas coordenadas pela Diretoria Geral de Segurança da Informação.

2. Definir os conhecimentos necessários ao desempenho da gestão da segurança da informação e providenciar os treinamentos necessários em todos os níveis da administração.

3. Elaborar a Política de Segurança da Informação.

4. Realizar ações corretivas emergenciais em função do risco iminente percebido nas etapas de mapeamento e de acordo com os critérios da Política de Segurança da Informação.

### 4.2.4. Implementar a Segurança.

Consiste em:

1. Divulgar corporativamente a Política de Segurança da Informação, tornando-a oficial e de conhecimento de todos, a fim de nortear as ações de todos os colaboradores sobre o manuseio, armazenamento, transporte e descarte de informação.

2. Coordenar a capacitação todos os colaboradores no manuseio, armazenamento, transporte e descarte de informação.

3. Implementar mecanismos de controle físicos, tecnológicos e humanos que irão permitir a eliminação das vulnerabilidades ou a sua viável administração a fim de manter o nível de risco em um patamar aceitável.

### 4.2.5. Administrar a Segurança.

Consiste em:

1. Monitorar os diversos controles implementados.

2. Garantir a legalidade.

3. Manter planos estratégicos para contingências e recuperação de desastres, objetivando o nível de disponibilidade adequado e a conseqüente continuidade operacional.

4. Manter os controles atualizados e realizar ações pró-ativas para mantê-las adequadas às novas mudanças requeridas pela evolução do ambiente interno e externo.

### 4.2.6. Garantir a Segurança nos Processos Administrativos e Legislativos.

Consiste em:

1. Sugerir alterações nos processos Administrativos e Legislativos para que sejam garantidos os níveis de segurança desejados.

2. Garantir que as medidas de segurança estabelecidas tenham o mesmo nível de qualidade em todos os processos da casa.

3. Estabelecer padrões para os fornecedores de produtos e serviços e realizar atividades de medição para verificar se os mesmos estão sendo atendidos.

A execução de cada etapa de modo correto permitirá ao Senado Federal reagir rapidamente às mudanças que ocorrerão e atuar adequadamente frente às oscilações dos riscos e das vulnerabilidades.

O PISI não finda quando a última etapa é realizada. Na verdade o Plano é constantemente realimentado e reiniciado, pois como sabemos as vulnerabilidades e riscos estão mudando de instante a instante e necessitam uma ação diuturna para garantir que os objetivos alcançados em um momento não sejam perdidos no momento seguinte.

## 4.3. GRUPO DE TRABALHO PARA PREPARAÇÃO DO PRODASEN PARA A NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Tendo em vista a renovação de um terço dos Senadores e a eleição de uma nova mesa Diretora para o biênio 2007-2008 que ocorrerá no início do próximo ano e os procedimentos burocráticos necessários para a implantação de órgão do nível de Diretoria Geral proposto neste estudo, bem como a criação das comissões, subsecretarias e assessorias recomendados a criação, no Prodasen, de um grupo de Trabalho para preparar a implantação da Nova Política de Segurança da Informação e realizar tarefas urgentes.

Este grupo de trabalho deverá utilizar como ponto de partidas as normas ABNT NBR ISO/IEC 17799:2005 e 27001:2006[5], o Manual de Boas Práticas em Segurança da Informação do TCU e a minuta de política de Segurança da Informação proposta neste estudo.

## 4.4. Atividades do Grupo de Trabalho de Segurança da Informação do Prodasen.

Sugerimos como atividades a serem realizadas pelo Grupo de Trabalho de Segurança da Informação do Prodasen as seguintes:

1. Analisar e, se for o caso, atribuir novas regras de acesso às áreas do Prodasen, observando controles de entrada e saída :

    1.1. de objetos pessoais;

    1.2. de dispositivos de armazenamentos portáteis, câmaras fotográficas, gravadores digitais e equipamentos multifuncionais;

    1.3. de volumes transportados à mão, em carrinhos e em veículos;

2. Analisar e, se for o caso, atribuir novas regras de acesso de pessoas às áreas do Prodasen.

3. Analisar e, se for o caso, propor alteração para a classificação de sigilo de documentos.

4. Apoiar a área de desenvolvimento para modernizar o sistema de controle de acesso e permissões únicos integrado com o sistema de Recursos Humanos.

5. Apoiar a área de infra-estrutura para angariar mais recursos para os ambientes de testes, homologação e recuperação de desastres.

6. Aprofundar o levantamento e o estudo das normas relacionadas no capítulo 3 deste estudo incluindo normas internacionais relevantes.

7. Atualizar a Política de Segurança da Informação do Prodasen.

8. Buscar consultoria externa para orientar as atividades de segurança da informação.

9. Conscientizar os níveis gerenciais sobre a responsabilidade de cada um no processo de implementação de uma Nova Política de Segurança da Informação.

10. Elaborar apostilas para uso seguro da TI.

11. Elaborar termos de responsabilidade para o uso seguro dos recursos de TI.

12. Estudar a aplicação da política de mesa limpa, tela limpa e quadro branco limpo.

13. Implementar medidas de descarte adequado a cada tipo de mídia.

14. Iniciar o mapeamento de ativos, riscos e vulnerabilidades no Senado Federal, atuando junto à Mesa Diretora para a adoção de medidas emergenciais.

15. Mapear os ativos, riscos e vulnerabilidades no âmbito do Prodasen e propor ao Diretor Executivo medidas de correção.

16. Pesquisar em outros órgãos de governo as Políticas de Segurança da Informação e os casos de sucesso com vistas a aproveitar a experiência adquirida.

17. Propor a aplicação de medidas educativas e disciplinares ou sanções contratuais aos infratores das normas de segurança.

18. Propor a atualização da metodologia de avaliação de sistemas adquiridos de terceiros.

19. Propor a atualização da metodologia de desenvolvimento de sistemas do Prodasen de acordo com as recomendações da norma ISO 17799.

20. Propor a atualização das normas obsoletas.

21. Propor a criação da Subsecretaria de Segurança da Informação no Prodasen, com sua estrutura, missão e atribuições.

22. Propor a criação de um procedimento/sistema para manter a Diretoria do Prodasen informada sobre os incidentes de segurança.

23. Propor atualização dos procedimentos de controle de instalação de softwares e de auditoria dos microcomputadores utilizados na rede do Senado.

24. Propor atualização dos contratos de prestação de serviços com a inclusão de clausulas de confidencialidade. Ver artigo de Rodrigo B. Fontoura [6] no anexo II deste estudo.

25. Propor atualizações nos processos de auditoria de sistemas do Prodasen.

26. Propor minutas padrão para os novos contratos de prestação de serviço incluindo clausulas de confidencialidade e padrões de segurança da informação a serem adotados.

27. Propor processos para auditoria periódica dos equipamentos móveis disponibilizados aos usuários.

28. Incluir no Termo de Responsabilidade de entrega de equipamentos móveis, recomendações de segurança da informação.

29. Treinar funcionários e colaboradores do Prodasen em segurança da informação, com ênfase em ataques de engenharia social.

30. Treinar os usuários do Senado sobre no uso seguro de TI.

## 4.5. NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Como produto do presente estudo apresentamos, no anexo I, uma minuta para a Nova Política de Segurança da Informação para o Senado Federal seguindo as orientações das já citadas normas ISO 17799 e 27001.

# 5. CONCLUSÃO

## 5.1. DIFICULDADES ENCONTRADAS NA ELABORAÇÃO DESTE ESTUDO

Durante a elaboração deste estudo encontramos situações que tornaram difícil a realização desta atividade embora tenhamos recebido apoio da alta direção do Prodasen para consecução do estudo. Dentre as dificuldades encontradas destacamos as seguintes:

1. Falta de disponibilidade de tempo para entrevistar pormenorizadamente todos os responsáveis pelas diversas áreas do Senado cujas atividades envolvem (ou podem envolver) a segurança da informação. Isto ocorreu devido às atividades que nós entrevistadores e os entrevistados temos que realizar em função das atribuições cotidianas no Senado Federal.

2. Em algumas entrevistas com servidores, principalmente da Subsecretaria de Infra-estrutura de Tecnologia, estabelecemos um contato maior, porém determinadas questões não foram detalhadamente respondidas visto que não somos funcionários da área de segurança do Prodasen, gerando conseqüentemente alguma reserva em aprofundar determinados temas.

3. Houve alguma dificuldade de acesso a toda documentação do Prodasen sobre segurança da informação, por razões de segurança, uma vez que não fazemos parte da equipe responsável pela segurança da informação do órgão.

4. A pesquisa na legislação interna do Senado Federal sobre Segurança da Informação foi complicada uma vez que não existe uma área que centralize toda a legislação / documentação embora existam sistemas onde isso pode ser feito. Todos os sistemas de recuperação da legislação apresentam deficiência nas ementas. Nas normas que possuem ementas algumas não possuem texto elucidativo. Tudo isso obrigou a uma extensa leitura das normas para verificar se o assunto se aplicava à Política de Segurança da Informação. Falta também nos sistemas, informações sobre a vigência das Resoluções e Atos, sendo necessário a análise de praticamente todas as normas.

## 5.2. Ações necessárias para implantação da Política de Segurança da Informação no Prodasen

Para a implementação da Política de Segurança da Informação no Prodasen as seguintes medidas deverão ser adotadas:

1. Apresentação do presente estudo à Diretoria do Prodasen com o objetivo de mostrar a relevância do assunto e a necessidade de revisão das normas vigentes. Isto também se faz necessário para que obtenhamos o comprometimento e apoio ostensivo da Direção conforme mencionado na alínea 2 do item 1.5. “Fatores críticos para o Sucesso” desta monografia.

2. Aperfeiçoar o presente estudo com o envolvimento efetivo de todas as áreas responsáveis pela segurança da informação.

3. Elaborar uma Sistemática de Gestão de Segurança da Informação seguindo as recomendações da norma ABNT NBR ISO/IEC 27001:2006.

# REFERÊNCIAS BIBLIOGRÁFICAS


[1] ABNT NBR ISO/IEC 17799:2005 – Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Código de Prática para a gestão da segurança da Informação.

[2] SÊMOLA, M.: Gestão da Segurança da Informação, Rio de Janeiro, Elsevier, 2003 – 5ª impressão.

[3] Meirelles, H. L.: Direito Administrativo Brasileiro, Editora Malheiros, 2006, 32º edição.

[4] Brasil. Tribunal de Contas da União: Boas práticas em segurança da informação, Brasília, TCU, 2003.

[5] ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos.

[6] Fontoura, R. B.: Os contratos de confidencialidade no Brasil. Acessado em 21/08/2006 em http://www.valoronline.com.br/valoreconomico/285/legislacaoetributos/legislacaoetributos/Os+contratos+de+confidencialidade+no+Brasil,,,86,3846062.html

# ANEXO I – NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

**ATO DA COMISSÃO DIRETORA Nº , DE**

*Regulamenta no âmbito do Senado Federal a Política de Segurança da Informação.*

**A COMISSÃO DIRETORA DO SENADO FEDERAL**, no uso de sua competência regimental e regulamentar, RESOLVE:

Art. 1º Aprovar a seguinte Política de Segurança do Senado Federal:

**"POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO SENADO FEDERAL**

**CAPÍTULO I – OBJETIVO**

**Art. 1º** Esta Política de Segurança da Informação estabelece diretrizes e padrões destinados a garantir os aspectos de autenticidade, integridade, confidencialidade, disponibilidade e legalidade das informações do Senado Federal.

**CAPÍTULO II – DIRETRIZES**

**Art. 2º** O Senado Federal assume que a informação é um bem da organização e deve ser protegida de ações não autorizadas de alteração, destruição ou divulgação, sejam elas acidentais ou intencionais.

**Art. 3º** A proteção da informação deve ser feita de forma preventiva e deve, também, permitir a sua pronta recuperação nos casos em que a proteção preventiva não tenha sido suficiente, independentemente dos meios físicos em que estejam armazenadas.

**Art. 4º** No âmbito do Senado Federal, todas as ações destinadas à proteção da informação devem sempre levar em consideração os aspectos físicos, tecnológicos e humanos inerentes ao assunto.

**Art. 5º** Todas as informações do Senado Federal, tratadas ou armazenadas em meio digital, devem ser protegidas com o uso de ferramentas automatizadas de apoio à

segurança da informação.

**Art. 6º** Todas as informações do Senado Federal, que não sejam tratadas ou armazenadas em meio digital, devem ser protegidas por meio de procedimentos adequados.

**Art. 7º** O direito de acesso à informação é decorrência da relação funcional ou determinação legal entre a pessoa e o Senado Federal, não constituindo prerrogativa da própria pessoa.

**Art. 8º** A qualidade dos Processos Legislativo e Administrativo do Senado Federal deve ser assegurada por informações corretamente protegidas, armazenadas e gerenciadas.

**Art. 9º** Os conceitos de Segurança da Informação devem ser incluídos nos programas de treinamento destinados a todos os servidores e colaboradores.

**Art. 10** Todos os contratos firmados que impliquem o manuseio de informações do Senado Federal devem conter cláusulas de proteção que garantam o cumprimento desta Política de Segurança da Informação.

**Art. 11** O cumprimento das disposições da Política de Segurança da Informação constitui condição de emprego e este fato deve fazer parte do documento de posse de servidores e de contratação de colaboradores.

## SEÇÃO I – CLASSIFICAÇÃO DA INFORMAÇÃO

**Art. 12** Toda informação deve ser classificada de acordo com o grau de importância que possui e também, em relação ao nível de sigilo necessário à preservação dos interesses da União.

**Art. 13** Todos os meios de armazenamento e de transporte de informações devem ser classificados de acordo com o mesmo nível de sigilo atribuído às informações neles armazenadas ou transportadas.

**Art. 14** Devem existir restrições de acesso às informações, de acordo com a classificação que lhes tenha sido atribuída.

## SEÇÃO II – SEGURANÇA LÓGICA

**Art. 15** Todo acesso à informação decorre de interesse do Senado Federal e deve ser registrado, indicando, no mínimo:

I. Qual a informação acessada;

II. Quem efetuou o acesso;

III. Qual a natureza do acesso;

IV. Quando se deu o acesso.

**Art. 16** Todo o desenvolvimento de aplicações e sistemas deve ser realizado em ambiente exclusivo, distinto do ambiente de produção, e fazendo uso, apenas, de massa de testes criada para tal finalidade. Não é admitido o uso de dados reais para teste de aplicações e sistemas em desenvolvimento bem como para treinamento.

## SEÇÃO III – SEGURANÇA FÍSICA

**Art. 17** Devem ser asseguradas todas as facilidades de infra-estrutura necessárias à manutenção da autenticidade, integridade, confidencialidade e disponibilidade da informação fundamental à continuidade das atividades legislativas e administrativas do Senado Federal, com especial destaque para o adequado e ininterrupto fornecimento de energia elétrica e o correto condicionamento de ar nas unidades responsáveis pela guarda e tratamento de informações.

**Art. 18** As unidades responsáveis pela guarda e tratamento de informações fundamentais à continuidade das atividades legislativas e administrativas do Senado Federal devem ser dotadas de eficientes sistemas de controle e monitoramento do acesso de pessoas aos seus ambientes.

## SEÇÃO IV – MICROINFORMÁTICA

**Art. 19** A contaminação e a disseminação de vírus de computador e outros programas ou códigos nocivos devem ser combatidas com o máximo empenho, sendo que os casos comprovadamente atribuíveis à má conduta dos usuários e estes poderão

responsabilizados penal, civil e administrativamente pelos danos que venham causar ao erário ou a terceiros.

**Art. 20** O Senado Federal está empenhado no combate à pirataria de software, em todas as suas formas, de modo que quaisquer casos eventualmente descobertos serão tratados de acordo com a legislação vigente no país que proíbe a pirataria de software, sem prejuízo das sanções penais, civis e administrativas cabíveis.

## SEÇÃO V – PLANO DE CONTINGÊNCIA

**Art. 21** Devem existir planos adequados à garantia da continuidade e à pronta recuperação das atividades legislativas e administrativas do Senado Federal, para os casos em que sinistros de qualquer natureza não tenham sido evitados pelas medidas preventivas de proteção.

**Art. 22** Toda informação fundamental à continuidade das atividades do Senado Federal devem possuir cópia de segurança guardada em local adequadamente protegido e distinto daquele em que se encontra a informação original.

## SEÇÃO VI – REDES

**Art. 23** O acesso à rede e aos sistemas do Senado Federal, seja por servidor ou não, a partir de equipamentos externos ao Senado, deve ser formalmente aprovado pela Secretaria Especial de Informática - Prodasen, de acordo com os Atos normativos em vigor.

**Art. 24** O acesso de servidor ou colaborador do Senado Federal a redes públicas de computadores deve ser restrito aos interesses da União e não admite qualquer manifestação em nome do Senado Federal.

**Art. 25** A interconexão da rede de computadores do Senado Federal a redes de outras organizações, públicas ou privadas, deve ser controlada e protegida contra invasões ou vazamento de informações.

# CAPÍTULO III – TIPOS DE USUÁRIOS

**Art. 26** Para os fins de proteção das informações, os usuários de recursos de informática desempenham um ou mais dos seguintes papéis:

I. **Gestor**: O gestor da informação é a maior autoridade na hierarquia organizacional, responsável pela criação da informação ou seu principal usuário, sendo que a gestão da informação pode ser compartilhada por dois ou mais gestores.

II. **Custodiante**: O custodiante da informação é a área ou o servidor responsável pelo processamento ou pela guarda da informação, o que não lhe confere acesso automático às informações custodiadas nem o direito de conceder acesso a terceiros.

III. **Auditor**: O auditor é o servidor que, no cumprimento das suas atividades, é responsável pelo controle e monitoramento da segurança das informações.

IV. **Usuário**: É toda pessoa autorizada a ter acesso à informação.

## CAPÍTULO IV – RESPONSABILIDADES

**Art. 27** São responsabilidades do gestor

I. Identificar as informações fundamentais ao funcionamento das atividades do Senado Federal relativas à sua área de atuação;

II. Classificar as informações sob sua gestão;

III. Estabelecer as regras de proteção que devem ser conferidas às informações;

IV. Autorizar o acesso de outros usuários às informações sob sua responsabilidade;

V. Acompanhar o cumprimento das regras de proteção estabelecidas;

VI. Decidir quanto a ação a ser tomada nos casos de tentativa ou de violação das regras de proteção;

VII. Responder pelos danos causados por ausência ou inadequação de regras de

proteção da informação;

VIII. Revisar periodicamente as regras de proteção estabelecidas.

IX. Elaborar o plano de contingência;

**Art. 28** São responsabilidades do custodiante

I. Orientar tecnicamente os demais usuários sobre aspectos relacionados à segurança da informação;

II. Recomendar ações visando reduzir possíveis fragilidades verificadas nas regras de proteção estabelecidas pelos gestores;

III. Implementar e administrar as regras de proteção definidas pelo gestor da informação;

IV. Detectar, identificar e comunicar ao gestor as tentativas ou violações de acesso não autorizado;

V. Participar da elaboração e implementar o plano de contingência;

VI. Revisar periodicamente as regras de proteção estabelecidas, em conjunto com o gestor da informação.

**Art. 29** São responsabilidades do auditor

I. Revisar a implementação das regras de proteção estabelecidas;

II. Avaliar a eficiência e a eficácia dos controles estabelecidos, notificando ao gestor as possíveis fragilidades encontradas;

III. Propor melhorias nas regras de proteção e nos controles estabelecidos.

**Art. 30** São responsabilidades do usuário

I. Usar a informação e todos os recursos a ela relacionados somente para os fins estabelecidos pelo gestor;

II. Cumprir as regras de proteção estabelecidas;

III. Manter sigilo sobre suas senhas de acesso aos sistemas e informações do Senado Federal;

IV. Responder por todo e qualquer acesso, bem como pelos efeitos dos acessos realizados com o uso do seu código de identificação e senha;

V. Alertar o gestor ou custodiante quanto a fragilidades encontradas no sistema ou nas regras de proteção estabelecida.

## CAPÍTULO V – RESPONSABILIZAÇÃO

**Art. 31** O comprovado não cumprimento dos termos desta Política de Segurança da Informação, por parte de qualquer servidor ou colaborador, sujeita o infrator às penalidades previstas na legislação vigente e penalidades contratuais.

**Art. 32** As empresas contratadas são co-responsáveis pelas ações de descumprimento das normas de segurança estabelecidas pelo Senado Federal, ficando também sujeitas às penalidades previstas na legislação vigente e penalidades contratuais.

## CAPÍTULO VI – VIGÊNCIA

**Art. 33** Esta versão da Política de Segurança da Informação entra em vigor a partir da data de sua publicação."

**Art. 2º** Este Ato entra em vigor a partir da data de sua publicação.

**Art. 3º** Revogam-se as ..... e demais disposições em contrário.

**SENADO FEDERAL**, de de

_____

Presidente do Senado Federal

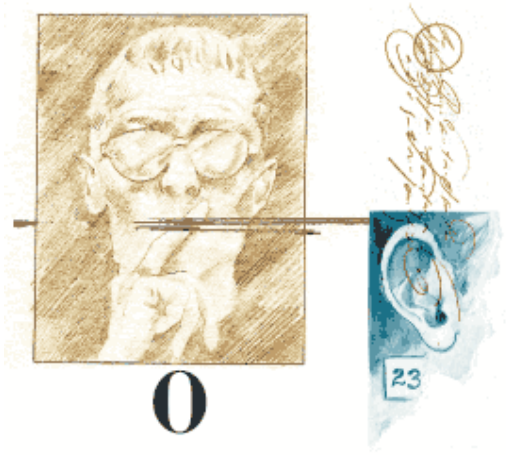
# ANEXO II – OS CONTRATOS DE CONFIDENCIALIDADE NO BRASIL

Publicado em Valor Econômico – Valor *Online* em 16 de agosto de 2.006.

*Por Rodrigo B. Fontoura*

## Os contratos de confidencialidade no Brasil

Os instrumentos de confidencialidade, nos dias de hoje, estão se tornando cada vez mais usuais quando o assunto em voga é prática jurídico-contratual, principalmente em âmbito corporativo. Neste sentido, praticamente toda intenção preliminar de negócio que envolva duas empresas vem acompanhada de uma manifestação formal de sigilo, mormente quando se trata de uma operação que envolva estudo, exclusividade e disputa concorrencial.




Destarte, muito em função do caráter globalizado inerente ao mundo corporativo de hoje em dia, os pactos jurídicos para a formalização de negócios no Brasil ganharam a influência dos instrumentos contratuais estrangeiros, principalmente os que se originam na doutrina jurídica do "*common law*", oriundos de países anglo-saxões, representados principalmente pelos americanos e britânicos.

Assim, sob a influência de nossos mais notórios investidores no país, os pactos negociais nacionais herdaram de seus irmãos globalizados a precaução jurídica

refletida nos "*non disclosure agreements*" - ou acordos de não-divulgação -, cujo objetivo principal seria o de evitar que as partes envolvidas em um negócio iminente, em andamento ou até mesmo potencial, pudessem utilizar o conhecimento desta operação sigilosa para, de alguma forma, prejudicá-la. Vale lembrar que esse poder de prejudicar o negócio decorreria do mau uso, pela parte que recebeu as informações sigilosas, do conhecimento das condições e/ou da operação em si, concretizado pela divulgação a terceiros, intencional ou não, daquilo que lhe foi divulgado.

Neste diapasão, adotou-se no Brasil, como prática jurídica de mercado para a realização de negócios estratégicos, a formalização de um pré-contrato de sigilo, usualmente conhecido como termo de confidencialidade, onde as partes obrigam-se a não divulgar determinadas informações consideradas sigilosas, concernentes a um negócio específico. Neste sentido, a utilização da informação sigilosa em qualquer situação que não a do negócio pretendido em si, cujo âmbito de circulação estaria restrito às partes, ficaria necessariamente vedada.

Até este ponto, tudo bem. Considerando-se, por óbvio, um mundo utópico, onde a teoria pudesse sobrepor-se à prática de mercado. Todavia, o que muitos não consideraram, no momento de fazer valer este peculiar sincretismo jurídico, foi exatamente o fato de existir uma grande diferença cultural e legislativa decorrente da própria origem de nosso direito pátrio em relação ao direito estrangeiro, criando lacunas legais.

Adotou-se no Brasil a formalização de um pré-contrato de sigilo, conhecido como termo de confidencialidade.

Assim, ainda que justificado pela ânsia de fazer valer uma nova e inovadora solução instrumental ou mesmo pela pressão de nossos parceiros estrangeiros - muitas vezes patrões e investidores - não se poderia simplesmente copiar um modelo de prevenção jurídico-contratual utilizado no direito estrangeiro e inseri-lo inconseqüentemente no direito brasileiro, sem que isto trouxesse seqüelas de validade e de aplicabilidade legal. E é neste tipo de lacuna que, nos contratos de confidencialidade, aparece o chamado "efeito espantalho".

O efeito espantalho é apenas um dos diversos nomes que poderíamos avocar para retratar uma mesma situação inerente aos contratos de confidencialidade praticados no Brasil: a falta das chamadas "*enforceable penalties*" - cláusulas penais que, por sua natureza dispositiva, possuem efetividade prática, fazendo-se valer de modo mais contundente do que as cláusulas penais remissivas, de natureza geral, que restam inócuas quando utilizadas neste tipo de pacto.

Neste sentido, como um espantalho que assusta apenas àqueles que desconhecem sua verdadeira natureza, as disposições penais atualmente consignadas nos contratos de confidencialidade praticados no Brasil costumam imputar à parte infratora, via de regra, apenas a responsabilidade pelas perdas e danos advindas de seu ato ou omissão, não possuindo aplicabilidade prática, dada a dificuldade natural de se provar a real extensão do dano decorrente da quebra do sigilo, o que, por conseqüência, significa não imputar qualquer responsabilidade. Fica, então, a constatação da realidade: se, por uma hipótese qualquer, a parte infratora violar o sigilo acordado, ficará sujeita apenas a uma ação judicial eivada de matérias de prova e de difícil comprovação.

Exatamente por isso, e objetivando superar o efeito espantalho, entendo que os contratos de confidencialidade devem sempre conter, em sua estrutura formal, cláusulas penais que possam imputar ônus pecuniário à contraparte, instituindo o dever de ressarcir independentemente da comprovação dos danos. É neste momento que a fixação de valores para o pagamento de uma multa contratual estipulada pela quebra da confidencialidade pode, em sede de pré-contrato, fazer a diferença fundamental entre o êxito de uma operação sigilosa, respaldado pelo temor de uma responsabilização efetiva, e o seu fracasso, corroborado pela impunidade de uma inexecução pactual.

Deste modo, fica como sugestão a utilização de cláusulas penais, em contratos de confidencialidade, que reflitam a pré-fixação de valores indenizatórios no caso de quebra do sigilo, devendo-se sempre levar em consideração que a adoção deste dispositivo terá o condão de minimizar os riscos atinentes à operação e, além disso, servirá ao potencial infrator como uma lembrança de que espantalho de casa também faz milagre.

Rodrigo B. Fontoura é advogado e consultor jurídico da CPFL Energia