UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE SEGURANÇA DA INFORMAÇÃO COM ENFOQUE NAS NORMAS DA ABNT NBR ISO/IEC 17799:2005 E NBR ISO/IEC 27001:2006 PARA APLICAÇÃO NO SENADO FEDERAL

KENDY APARECIDO OSIRO

ORIENTADORA: VERA PARUCKER HARGER

MONOGRAFIA DE ESPECIALIZAÇÃO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: UNB.LABREDES.MFE.007/2006

BRASÍLIA / DF: AGOSTO/2006

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE SEGURANÇA DA INFORMAÇÃO COM ENFOQUE NAS NORMAS DA ABNT NBR ISO/IEC 17799:2005 E NBR ISO/IEC 27001:2006 PARA APLICAÇÃO NO SENADO FEDERAL

KENDY APARECIDO OSIRO

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:

VERA PARUCKER HARGER, Especialista, UFRJ
(ORIENTADOR)

ROBSON DE OLIVEIRA ALBUQUERQUE, Mestre, UnB
(EXAMINADOR INTERNO)

ODACYR LUIZ TIMM, Mestre, Escola de Aperfeiçoamento de Oficiais do Exército - RJ
(EXAMINADOR EXTERNO)

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

FICHA CATALOGRÁFICA

OSIRO, KENDY A.
Estudo de Segurança da Informação com enforque nas Normas da ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal [Distrito Federal] 2006.
viii, 114 p., 297 mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2006).

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

1. Estudo de Segurança da Informação 2. Senado Federal
3. ABNT NBR ISO/IEC 17799:2005 4. ABNT NBR ISO/IEC 27001:2006

I. ENE/FT/UnB. II. Estudo de Segurança da Informação com enforque nas Normas da ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal [Distrito Federal]. 2006.

REFERÊNCIA BIBLIOGRÁFICA

OSIRO, A. K. (2006). Estudo de Segurança da Informação com enfoque nas Normas ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal. Monografia de Especialização, Publicação agosto/2006, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 114p.

CESSÃO DE DIREITOS

NOME DO AUTOR: KENDY APARECIDO OSIRO
TÍTULO DA DISSERTAÇÃO: Estudo de Segurança da Informação com enforque nas Normas da ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal.

GRAU/ANO: Especialista/2006.

Kendy Aparecido Osiro
SQSW 101, bloco I, ap. 104 - Sudoeste
CEP 70.670-109 – Brasília – DF - Brasil

Dedico este trabalho à minha esposa Arlene. Sem a sua paciência, apoio e incentivos – sejam por palavras, cafés e horas de sono este trabalho não poderia ser realizado.

AGRADECIMENTOS

À minha orientadora Profª. Vera Parucker Harger pelo constante apoio, incentivo, dedicação essenciais para o desenvolvimento deste trabalho e para o meu desenvolvimento como pesquisador.
Ao amigo, Prof. Timm da *Techsoft*, co-orientador deste trabalho, que apoiou e incentivou o autor na consecução deste trabalho.
A todos, os meus sinceros agradecimentos.
O presente trabalho foi realizado com o apoio do Unilegis – Universidade do Legislativo, órgão integrante da estrutura do Senado Federal destinado à promoção e manutenção de instituições e atividades voltadas ao aprimoramento dos procedimentos legislativos; da Alta Direção do Senado Federal e da Secretaria Especial de Informática – Prodasen, bem como da Faculdade de Tecnologia da Universidade de Brasília.

Estudo de Segurança da Informação com enforque nas Normas da ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal

RESUMO

O trabalho descrito nesta dissertação tem como objetivo estudar a importância da adoção de um Modelo de Gestão Corporativa de Segurança por parte do Senado Federal, com enfoque nas normas ABNT NBR ISO/IEC 17799 e ABNT NBR ISSO/IEC 27001:2006. Aborda como o Senado Federal vem trabalhando com questão da segurança em seu ambiente interno e publica uma pesquisa realizada entre os funcionários, terceirizados e estagiários acerca dessa questão. Ao final, sugere a adoção de algumas medidas que visam melhorar a Segurança da Informação no Senado Federal.

Study about Security of the Information with focus on the ABNT ISO/IEC 17799:2005 and 27001:2006, in order to apply in the Senate of Brazil.

ABSTRACT

The aim of this thesis is to study the importance of the adoption of a model of management of corporative security by the Senate of Brazil, with the focus on the ABNT ISO/IEC norms 17799:2005 and 27001:2006. It discusses how the Senate has been working with the security of the information in its inside environment and publishes a research done with employees on that issue. In its conclusion, it suggests the adoption of some measures in order to improve the security of the information in the Senate of Brazil.

ÍNDICE

Item **Página**

1. INTRODUÇÃO 1

2. CONCEITOS DE SEGURANÇA DA INFORMAÇÃO 3

2.1. O QUE É SEGURANÇA DA INFORMAÇÃO? 3

2.2. CRESCIMENTO DA DEPENDÊNCIA À INFORMATIZAÇÃO 4
2.2.1. Ciclo de Vida da Informação 6
2.2.2. Visão corporativa da Segurança da Informação 8

2.3. IDENTIFICANDO OS RISCOS 10
2.3.1. Avaliação, gerenciamento e análise de risco 10
2.3.2. Caracterização dos sistemas 13
2.3.3. Identificação das ameaças 14
2.3.4. Identificação das vulnerabilidades 14
2.3.5. O Jogo da Segurança 15

2.4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 17
2.4.1. Definição 17
2.4.2. Treinamento, publicação e divulgação 18
2.4.3. Utilização dos recursos de TI 20
2.4.4. Sigilo da informação 22
2.4.5. Autorização para uso dos recursos de tecnologia da informação 22
2.4.6. Estações de trabalho e servidores 23
2.4.7. Padronização das estações de trabalho e dos servidores 23
2.4.8. Formas de proteção 23
2.4.9. Estações móveis de trabalho 23
2.4.10. Termo de confidencialidade 24

2.5. PROTEÇÃO CONTRA SOFTWARE MALICIOSO 24
2.5.1. Vírus de computador 24
2.5.2. Softwares não autorizados 24
2.5.3. Procedimentos para acesso à Internet 25
2.5.4. Abrangência dos procedimentos de utilização dos recursos da Internet 26
2.5.5. Dicas para uma navegação segura 26

2.6. SEGURANÇA LÓGICA 27
2.6.1. Controle de acesso lógico 27
2.6.2. Processo de Logon 28
2.6.3. Senhas de acesso 29
2.6.4. Sistemas biométricos 30
2.6.5. Controle de Acesso à Rede 32
2.6.6. Combate a ataques e invasões 33
2.6.7. Privacidade das comunicações 35

2.7. SEGURANÇA FÍSICA E DO AMBIENTE 38
2.7.1. Acesso de funcionários e terceiros às dependências da organização 40
2.7.2. Controle de acesso físico 40
2.7.3. Controles ambientais 41
2.7.4. Segurança física de computadores pessoais 42
2.7.5. Investimentos em segurança física e ambiental 43

2.8. CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DA INFORMAÇÃO 44
2.9. ENGENHARIA SOCIAL 47
2.9.1. Engenheiro Social versus Security Officer 51
2.9.2. Solução Corporativa de Segurança da Informação 51
2.10. PROPOSTAS DE SEGURANÇA 52
2.10.1. Dificultando a Vida do Engenheiro Social 53
2.10.2. O que você sabe 54
2.10.3. O que você tem 55
2.10.4. O que você é 55
2.10.5. Plano de treinamento 56
2.10.6. Exemplos para Reforçar a Conscientização 58
2.10.7. Atuação do Security Officer 62
2.10.8. Penalidades e Processos Disciplinares 64
2.10.9. Conclusão 65
3. SEGURANÇA DA INFORMAÇÃO NO SENADO FEDERAL 67
3.1. VISÃO GERAL 67
3.2. PESQUISA SOBRE SEGURANÇA DA INFORMAÇÃO 69
4. REVISÃO DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO 86
4.1. Leis 86
4.2 Decreto nº 3.505/2000 87
4.3 NBR ISO/IEC 17799 (2000 e 2005) 88
4.3.1 ISO 27001:2005 [19] 89
4.3.2 Porque Adotar a NBR ISO IEC 17799:2005 [12] 91
4.3.3 A Nova Família das Normas ISO IEC 27000 91
5. CONCLUSÕES 93
5.1 Dificuldades 94
5.2 Trabalhos Futuros 95
REFERÊNCIAS BIBLIOGRÁFICAS 96
GLOSSÁRIO 98
ANEXOS 99

ÍNDICE DE TABELAS

Tabela Página

Tabela 2.1 - Identificação de vulnerabilidades 15

ÍNDICE DE FIGURAS

Figura Página

Figura 2.1 – Onipresença da informação nos principais processos de negócio 4

Figura 2.2 – Os quatro momentos do ciclo de vida da informação.....8

Figura 2.3 – Tipos de níveis de segurança nas empresas 12

Figura 2.4 – Ambiente sem política de segurança 15

Figura 2.5 – Diagrama dos componentes da..... 20

Figura 2.6 - Imagem de um e-mail falso (scam).....50

Figura 3.1 – Local onde trabalha 70

Figura 3.2 – Classificação do funcionário.....71

Figura 3.3 – O que é Segurança da Informação? 71

Figura 3.4 – Preocupação com a segurança da informação.....72

Figura 3.5 – Política de Segurança da Informação no Senado.....72

Figura 3.6 – Controle de acesso físico às instalações.....73

Figura 3.7 – Controle de acesso físico às instalações.....73

Figura 3.8 – Plano de contingência 74

Figura 3.9 – Plano de contingência 74

Figura 3.10 – Plano de contingência 75

Figura 3.11 – Treinamento em Segurança da Informação 75

Figura 3.12 – Engenharia Social.....76

Figura 3.13 – Importância das informações no dia-a-dia 76

Figura 3.14 – Utilização de triturador/fragmentador de papéis 77

Figura 3.15 – Canal de divulgação sobre Segurança da Informação.....77

Figura 3.16 – Troca de senha periodicamente 78

Figura 3.17 – Compartilha senha? 78

Figura 3.18 – Executa arquivos anexados em e-mail?.....79

Figura 3.19 – Licenças de *softwares* 79

Figura 3.19 – Licenças de *softwares* 79

Figura 3.21 – *Download* de arquivo 80

Figura 3.22 – Backup.....81

Figura 3.23 – Backup.....81

Figura 3.24 – Backup.....82

Figura 3.25 – Trojan.....82

Figura 3.26 – fornecimento de dados pessoais em listas.....83

Figura 3.27 – controle de e-mail 83

Figura 3.28 – monitoramento de acesso à internet 84

Figura 3.29 – faixa etária 84

1. INTRODUÇÃO

Vivemos na era da informação e da tecnologia, iniciada no século XX. Em especial, o computador e a telecomunicação tiveram avanços significativos nas últimas décadas, o que ocasionou um grande impacto sobre o *modus vivendi* das pessoas. Com os órgãos públicos não foi diferente. A revolução tecnológica chegou de forma avassaladora e muitos dirigentes e servidores públicos não avaliaram as conseqüências advindas das mudanças tecnológicas. Se por um lado a tecnologia facilitou o acesso e manuseio da informação, tornando mais rápida sua disseminação, por outro aumentaram os riscos de invasão de privacidade, integridade dos dados e a disponibilidade dos recursos tecnológicos. Estamos cada vez mais dependentes da tecnologia: um pane no sistema de informática pode redundar em prejuízos às empresas públicas e privadas, ocasionar prejuízos ao erário público, indisponibilizar serviços à população; fraudes podem ocorrer *on-line* e acarretar prejuízos incalculáveis às instituições públicas e privadas. Uma falha na segurança da informação resulta em danos não só monetários mas também morais.

O Senado Federal, órgão do Poder Legislativo, constitui um dos pilares da democracia. Sua missão principal é legislar e fiscalizar as ações do Poder Executivo e, para tanto, necessita de informação para a tomada de decisões. O que ocorreria se um projeto de lei, antes de ir à Plenário para votação, fosse alterado por pessoas não autorizadas. Qual seria o prejuízo decorrente dessa falha no sistema de informação? Difícil de se avaliar monetariamente, mas a imagem do Senado poderia ser seriamente afetada.

Para diminuir os riscos, há que se falar em investimento na segurança da informação. Isso por que a informação é um ativo, um dos maiores bens na atualidade, e como tal pode-se agregar valor à ela. Muitas pessoas pensam que Segurança da Informação se resume à compra de equipamentos e *softwares* caros, como *firewals*, sistema de detecção de intrusos ou antivírus. Outras acham que incluir a adoção de Políticas de Segurança e o estabelecimento de responsabilidades funcionais ao aparato tecnológico é suficiente. Mas nenhuma dessas abordagens consegue prevenir perdas se forem adotadas de forma isolada e inconseqüente.

O Novo Código Civil traz maior responsabilidade para os administradores de empresas e autoridades do Governo. O tema Segurança da Informação não está restrita apenas à área de Tecnologia da Informação (TI), mas se aproxima cada vez mais da atividade-fim e dos executivos da organização. Assim, os envolvidos com o processo de segurança devem se

interagir cada vez mais com os setores de TI, Auditoria, Jurídico, Recursos Humanos e Comunicação.

Este trabalho tem como objetivo estudar a importância da adoção de um Modelo de Gestão Corporativa de Segurança por parte do Senado Federal e tem enfoque na norma ABNT ISO/IEC 17799. Os capítulos de 2 a 8 tratam sobre os seguintes assuntos: importância da segurança da informação, riscos, Política de Segurança da Informação, Segurança Lógica, Segurança Física e do Ambiente, Classificação da Informação e Controle dos Ativos e Engenharia Social. O capítulo 9 faz uma análise geral de como o Senado Federal vem procedendo acerca da Segurança da Informação em seu ambiente interno. O capítulo 10 trata das normas pertinentes ao assunto. Por fim, o último capítulo, denominado conclusões, discorre sobre as dificuldades encontradas pelo autor para realização do presente trabalho, sugere a adoção de algumas medidas que visam melhorar a segurança da informação no Senado Federal e faz uma conclusão final sobre o presente trabalho.

2. CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

2.1. O QUE É SEGURANÇA DA INFORMAÇÃO?

Segundo a Norma NBR ISO/IEC 17799 “a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida.” Dessa forma, a informação é um patrimônio da empresa, tem valor. A segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades.

Na sociedade da informação, ao mesmo tempo que as informações são consideradas os principais patrimônios de uma organização, estão também sob constante risco, como nunca estiveram antes. A sua perda ou roubo constitui um prejuízo para a organização e é um fator decisivo na sua sobrevivência ou descontinuidade. A informação é o sangue das organizações que flui por todos os processos do negócio e está sujeita a muitas ameaças, vulnerabilidades. O que aconteceria se uma empresa perdesse todas as informações relativas aos seus clientes, fornecedores ou mesmo sobre os registros funcionais dos seus empregados? Poderia ter sérios prejuízos ou mesmo descontinuar sua atividade.

Para o autor Marcos Sêmola [1], “Segurança da Informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.” Segundo o autor, a expressão “Segurança da Informação” é ambígua, podendo assumir dupla interpretação.

1) Segurança como prática adotada para tornar um ambiente seguro.

2) Resultado da prática adotada.

Segundo o Manual do TCU [2], a segurança da informação visa garantir:

a) **confidencialidade**: garantia de que a somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento;

b) **integridade**: é a fidedignidade as informações. Pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital;

c) **disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem de direito.

d) **autenticidade**: Consiste na veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

Ferreira e Araújo [3], mencionam ainda os seguintes conceitos aplicados à segurança da informação:

e) **Legalidade**: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos;

f) **Auditabilidade**: o.acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;

g) **Não repúdio**: o usuário que gerou ou alterou a informação (arquivo ou e-mail) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

2.2. CRESCIMENTO DA DEPENDÊNCIA À INFORMATIZAÇÃO

Segundo Sêmola [1], a informação sempre esteve presente em todas as diversas fases da história e cumpre importante papel para a gestão do negócio. Todas empresas, independente de seu segmento no mercado, dependem e usufruem da informação, objetivando melhor produtividade, redução de custos, ganho de *market share*, aumento de agibilidade, competitividade e apoio à tomada de decisão.

NEGÓCIO		
Visão Sistêmica – Processos de Negócio	Visão Empresarial	**INFORMAÇÃO**
	Desenvolvimento de Negócios	
	Desenvolvimento de Soluções	
	Execução de Serviços	
	Gestão do Conhecimento	
	Apoio à Decisão	
	Aplicações	
	Infra-estrutura Física, Tecnológica e Humana	

Figura 2.1 – Onipresença da informação nos principais processos de negócio

Todo elemento que compõe os processos que manipulam e processam a informação, a contar com a própria informação, é um ativo. Assim, constitui ativo os equipamentos na qual a informação é manuseada, transportada e descartada, bem como as aplicações, usuários, ambiente e processos. O termo ativo possui essa denominação, oriunda da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo necessita de proteção adequada.

Havia uma época em que as informações nas empresas eram armazenadas apenas em papel e a segurança era relativamente simples. Bastava colocar os documentos num local seguro e restringir o acesso físico àquele local. Porém as coisas mudaram. A utilização da Tecnologia da Informação para o processamento e armazenamento de dados introduziu novos riscos e aumentou a fragilidade das informações. Fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio, inundação, erros de usuários, problemas causados por vírus, cavalos de tróia, *hackers*, etc., colocam em jogo a segurança e disponibilidade da informação.

Cada vez mais as organizações são dependentes dos sistemas informatizados. Cresce a quantidade e a complexidade de sistemas computacionais que controlam os mais variados tipos de operações e o próprio fluxo de informações das organizações. A computação distribuída dificultou ainda mais a implementação de um controle de segurança eficiente. Aliado a essa complexidade, muitos sistemas de informação não foram projetados para serem seguros.

Bill Gates [4] afirmou que "Os negócios vão mudar mais na próxima década do que mudaram nos últimos cinqüenta anos". Ele diz que "O modo como você reúne, administra e usa a informação determina se você vai perder ou ganhar". A pergunta que surge nessas afirmações é se o nosso ambiente está evoluindo junto com a complexidade das tecnologias que tratam a informação?

Ao analisar a evolução de como as empresas usavam a informação para gerir seus negócios, percebe-se que houve uma nítida mudança nas ferramentas com o passar dos anos. Alguns anos atrás, as informações eram tratadas de forma centralizada e pouco automatizadas. A informática engatinhava e os primeiros computadores eram grandes e caros. Em seguida, vieram os terminais burros, que serviam de consultas aos *mainframes*, que tinham a função central de processamento e armazenamento de dados.

Com o advento dos *chips* e microprocessadores, a capacidade de processamento tornou-se espantosa. De fato, Gordon Moore, um dos fundadores da *Intel Corporation*, constatou que a cada dezoito meses a capacidade de processamento dos computadores dobra, enquanto os custos permanecem constantes. Isto é, daqui a um ano e meio pode-se comprar um chip com o dobro da capacidade de processamento pelo mesmo preço que se paga hoje. Essa profecia ficou conhecida como Lei de Moore e ainda não parece ter prazo de validade definido.

O barateamento dos computadores e periféricos fizeram com que as empresas aplicassem como nunca a tecnologia da informação ao negócio, permitindo altos níveis de conectividade e compartilhamento. Dessa forma, a rede corporativa ganhou performance e o acesso à informação chegou a nível mundial pela rede mundial de computadores Internet. Novas expressões e aplicações comerciais surgiram com o advento da Internet, dentre elas podemos citar *business-to-business*,[1] *business-to-consumer*, *business-to-government*, *e-comerce*, *e-procurement*, e os sistemas integrados de gestão ERP – *Enterprise Resource Planning* que prometem melhor organização dos processos da organização.

2.2.1. Ciclo de Vida da Informação

Conforme explanado anteriormente, toda informação é influenciada por três propriedades principais: Confidencialidade, Integridade e Disponibilidade, além dos aspectos Autenticidade e Legalidade, que complementam esta influência.

Segundo Sêmola [1], o ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação que a colocam em risco. São quatro os momentos do ciclo de vida que são merecedores de atenção:

Manuseio

É o momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações num processador de texto, ou mesmo utilizar sua senha em um sistema de acesso, por exemplo.

[1] Vide glossário para esses e outros termos técnicos.

Armazenamento

Momento em que a informação é armazenada, seja em um banco de dados, num pedaço de papel ou numa mídia de CD-ROM, por exemplo.

Transporte

Momento em que a informação é transportada, seja por e-mail, fax ou ainda ao falar ao telefone, por exemplo.

Descarte

Momento em que a informação é descartada, seja ao jogar na lixeira um material impresso, descartar um CD-ROM por apresentar defeito ou qualquer outra mídia.

Não basta garantir a segurança de três das quatro fases acima. É necessário que todo o ciclo de vida da informação seja assegurado. Imagine, por exemplo que um diretor de uma empresa receba uma informação estratégica confidencial. Esta informação é anotada em papel e armazenada em um cofre. No momento posterior, o diretor solicita que a secretária digite a informação sigilosa e a envie por correio eletrônico, utilizando um processo criptográfico de transmissão. Contudo, após ter sido completada a tarefa, a secretária não adotou os procedimentos adequados de descarte, ou seja, ela jogou o papel na lixeira sem qualquer critério e tratamento. Neste exato momento, instaurou-se uma vulnerabilidade de segurança. Esta falha de segurança pode ser objeto de exploração por parte de um funcionário de uma empresa concorrente que tenha objetivos obscuros e consiga obter o papel com a informação confidencial apenas vasculhando a lixeira. Comparamos esse exemplo à uma pessoa que, antes de sair para uma viagem de férias, calibrou três pneus e esqueceu o quarto vazio ou furado.

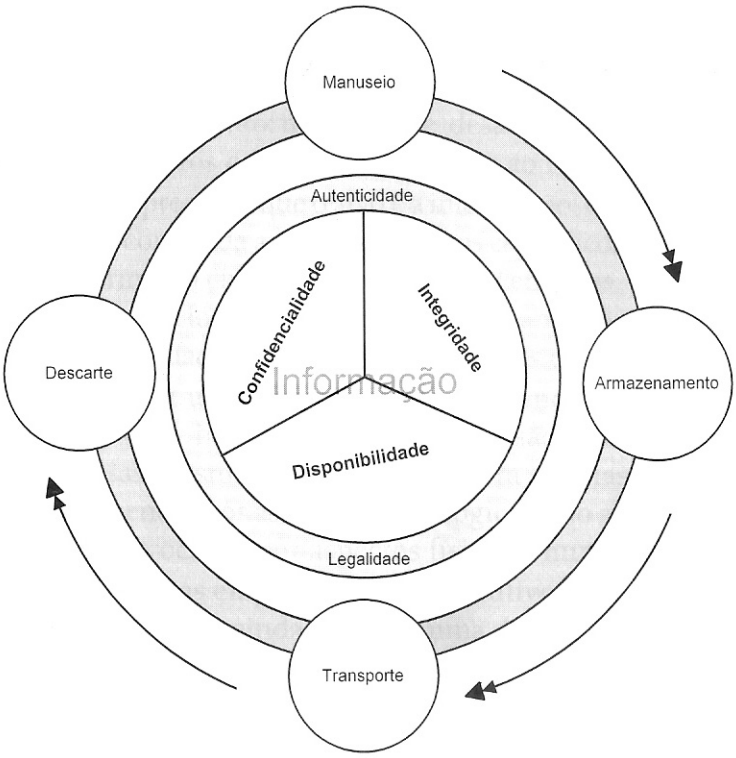


Figura 2.2 – Os quatro momentos do ciclo de vida da informação [SÊMOLA, 2003, p. 11]

Muitos executivos de empresas privadas e públicas vêem as ameaças associadas à segurança da informação como uma ponta de *iceberg*, ou seja, têm uma visão superficial do problema. As vulnerabilidades da informação transcendem os aspectos tecnológicos e também são provocadas por aspectos físicos e humanos.

2.2.2. Visão corporativa da Segurança da Informação

Faz-se necessário realizar ações que mapeiem e identifiquem a situação atual da instituição, seja ela pública ou privada, suas ameaças, vulnerabilidades, riscos, sensibilidades e impactos, a fim de permitir o adequado dimensionamento e modelagem da solução. O primeiro ponto a ser observado é que não existe risco zero. O que existe são vários níveis de segurança e cada nível está de acordo com a informação que se quer proteger e a natureza do negócio da empresa. Um alto nível de segurança pode gerar a perda da velocidade em função da burocratização de processos, insatisfação de clientes e fornecedores, até mesmo o desinteresse de investidores.

Conforme ensina Sêmola [1], a conscientização do corpo executivo da instituição é de extrema importância para o sucesso da melhoria da segurança por se tratar de um problema generalizado e corporativo, envolvendo aspectos físicos, tecnológicos e humanos que

sustentam a operação do negócio. Faz-se mister que se inicie o trabalho no formato *top down*, mobilizando os executivos da diretoria da empresa para depois atingir os demais na hierarquia. Isso se deve por não ser possível atingir simultaneamente todas as vulnerabilidades de todos os ambientes e processos da empresa, se não houver uma ação coordenada e principalmente apoiada pela cúpula.

O que vem a ser esse apoio? Além da sensibilização e da percepção dos executivos há também a conseqüente priorização das ações e definição orçamentária à altura. Mas por que eu preciso de segurança? A essa indagação, pode-se fazer uma comparação em relação a nossa vida cotidiana, em nosso lar: possuímos documentos, móveis, roupas, eletrodomésticos, automóvel, além de nossos familiares. Nessa situação, será que deixaríamos as portas e janelas abertas, sem nenhuma proteção? Claro que não. Mesmo que coloquemos trancas e alarmes em nossas portas, podemos dizer que nossa casa está segura? Será que falhas humanas podem ocorrer, como por exemplo empregados ou nossos familiares se esquecerem de ligar o alarme ou mesmo trancar adequadamente as portas, social e de serviço, quando saem de casa? Esse exemplo se aplica às instituições públicas e privadas. Não estaria a equipe de TI preocupada apenas com os aspectos tecnológicos de segurança e conseqüentemente esquecendo dos aspectos físicos e humanos? Será que os investimentos realizados em segurança estão alinhados com os objetivos estratégicos da empresa, a fim de propiciar o melhor retorno sobre o investimento? Suas ações estão orientadas por um Plano Diretor de Segurança ou continuam correndo de acordo com as demandas reativas em caráter emergencial? Estaria sua empresa operando em terreno de alto risco, encorajada por mecanismos de controle que lhe dão uma falsa sensação de segurança, apesar de continuar com as ‘portas trancadas’, mas as ‘janelas’ estão ainda abertas?

Cristiane Pereira [5], em seu artigo Atividades de Segurança da Informação, ensina:

> Falar sobre segurança é particularmente difícil quando o executivo da área é o único que está falando. Profissionais de segurança que não fizeram parcerias vitais com seus pares, nem implantaram iniciativas de educação que ampliem a base da responsabilidade pela segurança dificulta a implementação das estratégias que é conseguida por meio da gestão da segurança com a definição de um modelo de gestão de segurança corporativa, definindo papéis e atribuições para todos dentro da organização e isto significa tratar partes de seus problemas correntes como pacotes de trabalhos.

De fato, o problema de segurança é de responsabilidade de todos os funcionários da empresa, desde o executivo até o contínuo. Essa cultura só pode ser conseguida mediante a adoção de uma Política de Segurança, treinamento e atribuições de responsabilidades aos funcionários, bem como aplicação de sanções, quando houver atos de negligência ou má-fé.

Erros cometidos

Muitos são os erros praticados na hora de pensar em segurança da informação, decorrentes de uma visão míope do problema. Sêmola [1] destaca os seguintes erros comumente cometidos:

1. atribuir exclusivamente à área de tecnologia a segurança da informação.
2. posicionar hierarquicamente o Conselho de Segurança da Informação abaixo da diretoria de TI.
3. Definir investimentos subestimados e limitados à abrangência dessa diretoria.
4. Elaborar planos de ação orientados à reatividade.
5. Não perceber a interferência direta da segurança com o negócio.
6. Tratar as atividades como despesa e não como investimento.
7. Adotar ferramentas pontuais como medida paliativa.
8. Satisfazer-se com a sensação de segurança provocada por ações isoladas.
9. Não cultivar corporativamente a mentalidade de segurança.
10. Tratar a segurança como um projeto e não como um processo.

2.3. IDENTIFICANDO OS RISCOS

2.3.1. Avaliação, gerenciamento e análise de risco

Segundo a *Foco Security* [6], a Análise de Risco tem por objetivo identificar os riscos de segurança presentes na organização, fornecendo conhecimento para que sejam implementados controles eficazes de Segurança.

Apesar da segurança aparente dos ambientes críticos de uma organização e da competência de seus dirigentes, é perfeitamente possível que, dada a complexidade e a abrangência dos ambientes organizacionais, passem despercebidas vulnerabilidades que, se devidamente exploradas, representam risco para segurança de suas informações e do próprio negócio.

As características atribuídas ao gerenciamento de riscos em geral levam as ciências sociais em suas diversas disciplinas, a saber sociologia, antropologia, psicologia, história, etc. a se debruçarem sobre o tema, principalmente devido à necessidade de se compreender as

questões associadas aos riscos tecnológicos e do negócio. Segundo Edmir Moita [7], chefe da Assessoria de Gerenciamento de Riscos do Ministério da Previdência e Assistência Social, o termo "risco" deriva da palavra italiana "*riscare*", cujo significado original era navegar entre rochedos perigosos, e que foi incorporada ao vocabulário francês em torno de 1660. No entanto, o conceito mais contemporâneo origina-se da teoria das probabilidades e implica a consideração de predição de situações ou eventos por meio do conhecimento ou pelo menos possibilidade de conhecimento da potencialidade de perdas e danos e da amplitude de suas conseqüências. Neste contexto, risco pode ser definido como uma estimativa para as possíveis perdas de uma instituição qualquer, devido às incertezas de suas atividades cotidianas.

A abordagem científica do gerenciamento de riscos teve seu início nos Estados Unidos e em alguns países europeus, quando do estudo da possibilidade de redução de prêmios de seguros e a necessidade de proteção da empresa frente a riscos de acidentes. O que os americanos e os europeus na realidade fizeram foi aglutinar o que já se vinha fazendo de forma independente, em um conjunto de teorias as quais denominaram de *Risk Management*. A idéia principal que balizou o desenvolvimento deste conjunto de teorias refletiu tanto uma tendência para prever, planejar e alertar sobre os riscos, como a idéia de que as decisões regulamentadoras sobre os mesmos seriam menos controversas se pudessem ser estatisticamente comprovadas.

Ultimamente, o tema Gerenciamento de Riscos vem sendo amplamente discutido na academia, entretanto, não temos relatos de sua aplicação na administração pública. Cristiane Betanho [8] atenta para o fato de que *"uma empresa pública, normalmente, tem cultura diferenciada das empresas do mercado livre. Tem sua imagem pré-determinada pelo fato de que é pública. Tem funcionários cuja cultura encara a estabilidade como a não necessidade de mudanças, enquanto que deveria utilizá-la visando o desenvolvimento e a proteção da cidadania. Negando a necessidade de mudanças, a organização nega a presença de riscos."* A administração pública brasileira, por sua vez, não foge às características apresentadas pela referida autora.

Fazem parte de uma Análise de Risco:

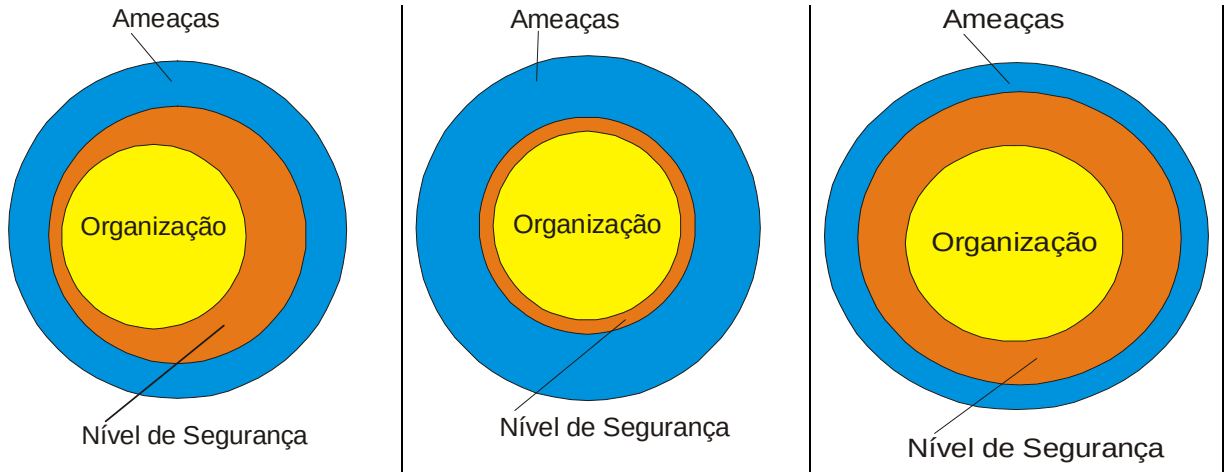
- **Processos de Negócio**: Identificar junto aos gestores e colaboradores os Processos de Negócio existentes na Empresa.
- **Ativos**: Identificar os ativos que serão considerados na Análise de Risco: Pessoas, Infra-estrutura, Aplicações, Tecnologia e informações.

- **Vulnerabilidades:** Identificar as vulnerabilidades existentes nos ativos que possam causar indisponibilidade dos serviços ou serem utilizadas para roubo das suas informações.
- **Ameaças:** Toda e qualquer condição adversa capaz de causar alguma perda para a organização. Uma ameaça é uma condição potencial. Ela não irá causar necessariamente um dano;
- **Desastre:** é o impacto de uma força externa agressiva que pode ocasionar perda ou prejuízo significativo. Necessariamente, um desastre não precisa ser destruidor. Em alguns casos, ele é apenas uma condição que impede a operação de uma atividade crítica, necessária para a geração de um serviço ou produto;
- **Impacto:** Tendo identificado as vulnerabilidades e ameaças, identificamos o impacto que estes podem causar na Empresa. Como roubo de informação, paralisação de serviços, perdas financeiras entre outros.

Alguns Benefícios

- Conhecimento dos riscos da Empresa.
- Otimização de recursos.
- Ter subsídios para um Plano de Ação

A Análise de Risco possibilita enquadrar a organização em uma das situações abaixo.



Nível de segurança bem implementado para algumas situações, porém outras extremamente fracas.	Nível de segurança fraco em todas as situações. Empresa não protegida	Nível de segurança bem implementado, homogêneo por todos os lados.

Figura 2.3 – Tipos de níveis de segurança nas empresas

Segundo Fernando Ferreira [9], para determinar a probabilidade de um evento, as ameaças existentes que cercam o ambiente de Tecnologia da Informação devem ser analisadas, bem como as vulnerabilidades potenciais e controles de segurança implementados e disponíveis.

O impacto é o resultado de um dano causado por uma ameaça, que explorou uma vulnerabilidade. O nível de impacto é determinado pelos aplicativos de missão crítica da organização e seus ativos de informação afetados. A metodologia de avaliação de riscos contempla nove passos que, obrigatoriamente, devem ser seguidos:

2.3.2. Caracterização dos sistemas

Para conduzir a avaliação de riscos em ambientes informatizados deve-se primeiramente definir seu escopo e abrangência. Neste passo, as limitações dos sistemas são identificados por meio de recursos e informações que os constituem. Caracterizar um sistema informatizado ajuda na definição do escopo e abrangência, delineia os limites para autorizações e fornece informações essenciais para definir o risco. Identificar risco em sistemas informatizados requer uma grande compreensão do seu ambiente de processamento. Os responsáveis pela condução da avaliação de riscos devem coletar as seguintes informações relacionadas aos sistemas sob análise: hardware, software, interfaces (internas ou externas), dados e informações, pessoas que fornecem suporte e utilizam os sistemas; missão do sistema; criticidade dos dados e sistemas, ou seja, nível de proteção necessária para garantir a integridade, disponibilidade e confidencialidade dos dados.

No entendimento de Mário Peixoto [10], deve-se ter em mente que o alicerce que assegura os princípios básicos da segurança da informação, confidencialidade, integridade e disponibilidade, tem de levar em conta três aspectos: a segurança física, a segurança tecnológica e a segurança humana.

A coleta de informações sobre os sistemas informatizados pode ser realizada por meio de: questionários para o pessoal técnico e gerência responsável pelo desenvolvimento ou suporte do sistema; entrevista dos funcionários que lidam com os sistemas; revisão da documentação, que podem fornecer importantes informações sobre os controles de segurança utilizados e planejados para o sistema; e utilização de ferramentas automatizadas, ou seja, *softwares* específicos podem ser utilizados para obtenção de informações adicionais, ou para confirmar a existência da utilização de controles de segurança. Um exemplo poderia ser uma

ferramenta de mapeamento de rede que pode identificar serviços que estão sendo executados, diagnosticar as políticas de segurança em uso, etc.

2.3.3. Identificação das ameaças

Ameaça é a possibilidade de um invasor ou evento inesperado explorar uma vulnerabilidade de forma eficaz. Vulnerabilidade é uma fraqueza que pode ser acidentalmente utilizada ou intencionalmente explorada. Uma fonte de ameaça não representa riscos quando não existe vulnerabilidade que possa ser utilizada. O primeiro passo é a identificação das fontes de ameaça, destacando-se as ameaças que são aplicáveis ao ambiente avaliado.

Ela é definida como qualquer circunstância ou evento que pode causar danos aos sistemas informatizados. As ameaças mais comuns são as causas naturais, falhas humanas ou ambientais. Por exemplo, embora a probabilidade de inundação natural de um ambiente informatizado localizado no deserto seja baixa, deve-se considerar a ameaça do rompimento de um encanamento. Os funcionários podem ser considerados como potenciais fontes de ameaças por meios de atos intencionais devido ao seu descontentamento com a organização, ou atos não intencionais como negligência e erros. Um ataque pode ser uma tentativa maliciosa de obter acesso não autorizado a um sistema podendo comprometer a integridade, disponibilidade, e confidencialidade das informações ou somente para obtenção de acesso para efetuar algum tipo de consulta ou suporte, mas burlando a segurança.

2.3.4. Identificação das vulnerabilidades

A análise de uma potencial ameaça em um sistema informatizado deve obrigatoriamente incluir a determinação das vulnerabilidades associadas ao seu ambiente. O objetivo desta etapa é desenvolver uma relação das vulnerabilidades do sistema (falhas ou fraquezas) que podem ser exploradas pelas potenciais fontes de ameaça. Ex.:

Vulnerabilidade	**Fonte de ameaça**	**Ações utilizadas**
Os User Ids dos usuários demitidos não são removidos do sistema.	Usuários demitidos.	Tentativas de acesso remoto à rede para acessar informações da organização.
O *firewall* aceita *Telnet* e os usuários do tipo convidado estão ativos no servidor	Usuários não autorizados	Utilização do *Telnet* no servidor utilizando o usuário do tipo convidado para obter informações
O fabricante identificou e publicou as fraquezas de segurança relacionadas ao seu sistema aplicativo. Entretanto,	Usuário não autorizados.	Obtenção de acesso não autorizado aos sistemas e informações confidenciais, baseados na vulnerabilidade

Vulnerabilidade	Fonte de ameaça	Ações utilizadas
os respectivos *patches* de segurança não foram aplicados		divulgada.

Tabela 2.1 - Identificação de vulnerabilidades

Os métodos recomendados para identificação das vulnerabilidades dos sistemas são a utilização de fontes ou repositórios de vulnerabilidades, o resultado dos testes de performance dos sistemas e o desenvolvimento de *checklists* de segurança.

2.3.5. O Jogo da Segurança

A empresa *Modulo Security Solutions* [11], líder em Segurança da Informação na América Latina, trouxe, dentre inúmeros outros artigos que sempre divulga em seu portal, um documento muito interessante e bastante didático desenvolvido pelo *Modulo Education Center*, relativo à Segurança da Informação no ambiente corporativo. Na figura abaixo, há inúmeras falhas de segurança no ambiente físico, técnico e humano.

Figura 2.4 – Ambiente sem política de segurança [MODULO SECURITY]

Dentre as inúmeras falhas que podem ser observadas na figura, muitas são simples de serem resolvidas, seguindo políticas de segurança e condutas educativas por parte dos funcionários da empresa. Vejamos os erros:

1 – mencionar senha por telefone. Esta informação não deve ser mencionada por este meio e antes de disponibilizar qualquer tipo de informação, deve-se certificar com quem fala, de onde fala, conferir a origem da ligação e por que o interlocutor quer a informação.

2 – Visitantes terem acesso à área interna na empresa, obtendo contato com as informações confidenciais, sem estar devidamente autorizado e identificado.

3 – Entrega de informações digitais (disquete, CD, etc.), sem o prévio conhecimento da procedência e da inspeção do material recebido que possa comprometer a organização.

4 – Descarte incorreto de material que se acha inútil jogado no lixo, sem o picotamento.

5 – Cabos e fios que interligam os computadores soltos no meio da sala, sem a devida organização de estarem atrás do micro salvaguardado de qualquer tropeço ou acidente.

6 – Gavetas abertas, de fácil acesso a documentos.

7 – Jogos via internet ou mesmo por disquetes ou CD-ROM são passíveis de conter armadilhas, como ativação de *worms*, cavalos de tróia, vírus dentre outros perigos que se escondem por trás dos jogos ou diversões oferecidas na internet.

8 – arquivos de *backup* expostos. Estes devem ser guardados em lugar seguro e confiável.

9 – Nome de usuário e senha afixados em local público.

10 – Fumar em ambiente de trabalho, podendo ocasionar incêndio no carpete.

11 – Computador ligado demonstrando informações confidenciais como senha, usuário, códigos fontes.

12 – Acesso a *sites* indevidos, não confiáveis, ou fora das políticas de trabalho da empresa.

13 – Sistema de alarme desativado, desligado ou inoperante, em caso de alguma urgência ou emergência.

2.4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.4.1. Definição

Segundo Ferreira e Araújo [3], a Política de Segurança da Informação (PSI) pode ser definida como conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação. O objetivo da PSI é “Prover à direção uma orientação e apoio para a segurança da informação” ISO/IEC 17799.

Segundo a Norma ISO/IEC 17799 [12], sugere a aprovação e publicação da PSI pela direção, bem como a sua comunicação de forma adequada, para todos os funcionários da empresa. Os seguintes aspectos devem ser observados:

- Estabelecimento do conceito de que as informações são um ativo importante da organização;
- Envolvimento da Alta Administração com relação à Segurança da Informação;
- Responsabilidade formal dos colaboradores da empresa sobre a salvaguarda dos recursos da informação, incluindo os registros de incidentes de segurança;
- Estabelecimento de padrões para a manutenção da Segurança da Informação.

De acordo com Ferreira e Araújo[3], é essencial definir claramente o escopo da PSI, já que ela pode abranger apenas alguns serviços e áreas da organização. Conforme foi explanado anteriormente, não deve se ater apenas a *hardware* e *software* que compõem os sistemas, e sim abranger também, as pessoas e os processos de negócio. Assim, considera-se o *hardware*, *software*, dados e documentação, identificando de quem estes elementos necessitam ser protegidos. Os autores ressaltam que as políticas, normas e procedimentos de segurança devem ser:

1) Simples e compreensível: deve ser de fácil leitura, com uma linguagem simples, clara, concisa e direta, evitando termos técnicos de difícil entendimento.

2) Homologadas e assinadas pela Alta Administração: o nome do dirigente principal da organização deve constar do documento, demonstrando que está de acordo com as políticas expostas no documento, bem como mostra seu comprometimento para que elas sejam adequadamente cumpridas.

3) Estruturadas de forma a permitir a sua implementação por fases;

4) Alinhadas com as estratégias da organização, padrões e procedimentos já existentes: em muitas organizações é comum que as políticas em vigor façam referência a outros regulamentos internos já existentes ou em desenvolvimento.;

5) Orientadas aos riscos;

6) Flexíveis, ou seja, moldáveis aos novos requerimentos de tecnologias e negócio;

7) Proteger os ativos de informações, priorizando os de maior valor e de maior importância;

8) Positivas e não apenas concentradas em ações proibitivas ou punitivas.

É altamente recomendado que se crie um Comitê de Segurança da Informação, que deve ser constituído por gerentes e diretores de diversos setores, como por exemplo, informática, jurídico, auditoria, engenharia, segurança, recursos humanos e outros que forem necessários. Além destes, há que se criar o papel do *Security Officer* (Oficial de Segurança), que são especialistas em segurança com a responsabilidade de planejar, organizar, executar e controlar atividades de segurança da informação.

A segurança pode ser desmembrada em quatro grandes aspectos:

- **Segurança computacional**: conceitos e técnicas utilizados para proteger o ambiente informatizado contra eventos inesperados que possam causar qualquer prejuízo.

- **Segurança lógica**: prevenção contra acesso não autorizado.

- **Segurança física**: procedimentos e recursos para prevenir acesso não autorizado, dano e interferência nas informações e instalações físicas da organização.

- **Continuidade de negócios**: estrutura e procedimentos para reduzir, a um nível aceitável, o risco de interrupção, ocasionadas por desastres ou falhas por meio da combinação de ações de prevenção e recuperação.

2.4.2. Treinamento, publicação e divulgação

A Política de Segurança por si só não garante a proteção dos ativos da empresa. Ela deve ser escrita em linguagem simples e divulgada por meio de avisos internos como, por exemplo, e-mail, comunicação interna, intranet, reuniões de conscientização, elaboração de material promocional sobre o esclarecimento dos principais pontos, reuniões de conscientização, etc. Outra forma de conscientizar os usuários é o treinamento direcionado.

De acordo com a norma técnica NBR ISO/IEC 17799 [12], seção sobre Treinamento dos Usuários, “deve-se garantir que os usuários estejam cientes das ameaças e das preocupações de segurança da informação e estejam equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho”. Dessa forma, todos os funcionários da organização devem receber treinamento apropriado e atualizações regulares sobre as políticas corporativas. Isso inclui requisitos de segurança, responsabilidades legais e controles do negócio, bem como treinamento sobre o uso correto dos recursos de Tecnologia da Informação como, por exemplo, procedimentos de acesso ou uso de pacotes de software antes que seja fornecido qualquer acesso aos serviços. O treinamento dos usuários resulta na conscientização das ameaças e das preocupações de segurança da informação e estão equipados para apoiar a política de segurança durante a execução de seu trabalho.

Punições devem ser estabelecidas e aplicadas a todos os funcionários, incluindo os estagiários, prestadores de serviço, colaboradores, etc., pelo não cumprimento da Política de Segurança. Devem ser definidas punições de acordo com a cultura da organização. Algumas empresas optam por criar níveis de punições relacionados aos itens da política, sendo a punição máxima a demissão. O principal objetivo de se estabelecer punições, pelo não cumprimento da Política de Segurança, é incentivar os usuários a aderirem à política, e também dar respaldo jurídico à organização.

Convém que todos os incidentes de segurança reportados através de canais apropriados o mais rápido possível. A notificação dos incidentes terão maior probabilidade de ocorrer se os funcionários forem treinados e tiverem consciência dos procedimentos.

A Política de Segurança deve capacitar a organização com instrumentos jurídicos, normativos e processuais. Esses instrumentos devem abranger as estruturas físicas, tecnológicas e administrativas, de forma a garantir a confidencialidade, integridade e disponibilidade das informações corporativas.

Desta forma, com o propósito de fornecer orientação e apoio às ações de gestão da segurança, a política possui uma função fundamental e assume uma grande abrangência, podendo ser subdividida em três blocos (vide figura 2.5):

• Diretrizes: possuem papel estratégico e devem expressar a importância que a organização dá aos ativos de informação, além de comunicar aos funcionários seus valores;

• Normas: segundo nível da política que detalha situações, ambientes, processos específicos e fornece orientação para o uso adequado das informações;

Procedimentos: está presente na política em maior quantidade por seu perfil operacional. Descrição detalhada sobre como atingir os resultados esperados.

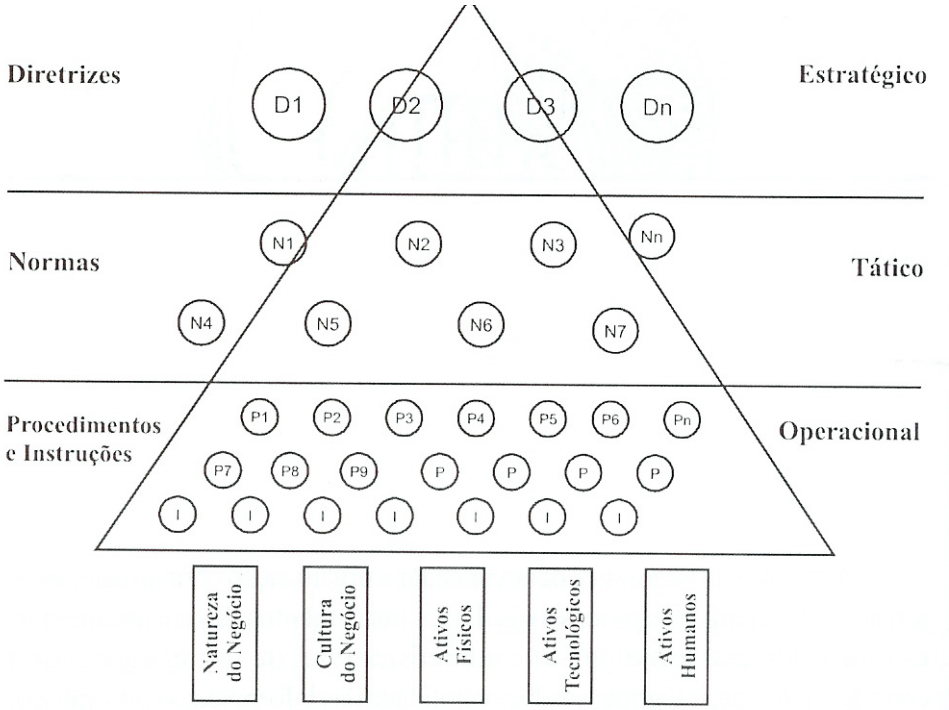


Figura 2.5 – Diagrama dos componentes da Política de Informática

2.4.3. Utilização dos recursos de TI

A utilização de recursos tecnológicos pelos colaboradores deve ocorrer apenas no desempenho de atividades diretamente relacionadas aos negócios da organização.

As políticas da organização não devem admitir o uso dos recursos para a discriminação ou provocação em razão do sexo, raça, cor, religião, nacionalidade, idade, porte de deficiência física, condição de saúde, estado civil ou qualquer outra condição prevista em lei. Adicionalmente, em nenhuma hipótese, os colaboradores poderão utilizar meios tecnológicos para transmitir, receber ou armazenar qualquer informação que seja discriminatória, difamatória ou provocativa (material pornográfico, mensagens racistas, piadas, desenhos etc.).

Sobre a violação de direitos autorais, os colaboradores não podem utilizar recursos tecnológicos da empresa para copiar, obter ou distribuir material protegido por direito autoral.

A organização deve somente disponibilizar recursos tecnológicos aos colaboradores (funcionários ou terceiros) autorizados de modo a auxiliá-los no desempenho de suas funções e na execução dos trabalhos.

A política deve ressaltar que cada colaborador é responsável por usar os recursos tecnológicos disponíveis de forma a aumentar sua produtividade e contribuir para os resultados e a imagem pública da organização.

Os colaboradores devem ser responsáveis pela guarda, zelo e bom uso dos recursos tecnológicos disponibilizados, conforme as instruções do fabricante e a Política de Segurança.

Ao desrespeitar a política da organização, no que diz respeito ao uso de seus recursos tecnológicos, o colaborador deve estar sujeito a medidas disciplinares.

A política deve assegurar que a organização detém todos os direitos, independentemente de seu conteúdo, sobre todos os dados e informações armazenados nos componentes do sistema de computação, bem como sobre as mensagens, dados e informações enviados e recebidos no sistema de correio eletrônico e correio de voz.

Portanto, a política deve contemplar aspectos onde se reserva o direito de acessar, a seu critério e a qualquer momento, todos os seus meios tecnológicos, incluindo computadores, sistema de correio eletrônico e de correio de voz. Tal situação deve estar suportada por um termo devidamente assinado pelo usuário.

Conforme atribuídas as responsabilidades, o usuário dos recursos tecnológicos é responsável pela segurança das informações da organização que estão sob sua responsabilidade.

A política deve ressaltar que determinados recursos tecnológicos da empresa podem ser acessados apenas mediante o fornecimento de uma senha válida, ou seja, as senhas são utilizadas para prevenir acessos não autorizados à informação e não conferem ao colaborador nenhum direito de privacidade.

Os colaboradores devem manter suas senhas como informação confidencial. Não deve ser permitido compartilhá-las, nem acessar sistemas de outros colaboradores sem autorização expressa, conforme a hierarquia interna de responsabilidade para autorizações e aprovações. Nesses casos, somente o diretor ou o gerente (responsável pelo funcionário), que tenha autorizado formalmente a quebra do sigilo de um colaborador, pode acessar essas informações, de modo a garantir o sigilo das demais informações.

Por medida de segurança, nenhum computador poderá utilizar conexões discadas para acesso à Internet ou outros serviços de informação quando conectados à rede da organização.

Os colaboradores que tentarem burlar ou desabilitar os dispositivos de segurança, que asseguram a integridade dos recursos tecnológicos da organização, devem estar sujeitos a ações disciplinares.

2.4.4. Sigilo da informação

A questão da proteção de segredos do negócio e outros tipos de informação confidencial, ou de titularidade tanto da organização quanto de seus parceiros de negócio, deve ser tratada com extrema relevância.

Não deve ser autorizada a transmissão de informação confidencial por meios eletrônicos para destinatários fora dos domínios da organização.

Deve-se definir claramente para os colaboradores quais dados, assuntos etc. são confidenciais e merecem tratamento especial.

A transmissão de informações classificadas como "confidenciais" dentro da rede da organização requer aprovação do diretor ou do gerente. Sempre que possível, a área de Segurança da Informação deve providenciar para seus usuários meios eletronicamente seguros para a transmissão e o arquivamento das informações e dados classificados como "confidenciais".

As políticas devem considerar que "meio eletronicamente seguro" é a transmissão de dados criptografados através de uma rede privada de dados (VPN - *virtual private network*). Neste caso, em nenhuma hipótese o código de acesso (ou chave do código) poderá ser transmitido junto com os dados confidenciais.

2.4.5. Autorização para uso dos recursos de tecnologia da informação

O acesso a recursos tecnológicos deve ser concedido exclusivamente com base em critérios estabelecidos pela organização.

Como regra geral, o acesso deve ser concedido levando em conta a função desempenhada pelo colaborador. As autorizações e aprovações necessárias para o cumprimento dos procedimentos e instruções de trabalho devem ser fornecidas conforme a hierarquia de responsabilidades exemplificadas a seguir:

- Diretor: poderá efetuar autorizações e aprovações necessárias para os diretores e gerentes sob sua subordinação direta;
- Gerente: poderá efetuar autorizações e aprovações necessárias para os gerentes, chefes, encarregados e demais colaboradores sob sua subordinação direta.

2.4.6. Estações de trabalho e servidores

As estações de trabalho e servidores são essenciais para a realização de qualquer atividade. As políticas devem especificar que os equipamentos e recursos tecnológicos são de uso restrito da organização. Devem estar em local seguro, ter acesso restrito e protegido contra desastres com um nível de segurança proporcional à importância do bem e das informações neles contidas.

2.4.7. Padronização das estações de trabalho e dos servidores

A organização deve classificar as estações e os servidores identificando a finalidade de cada equipamento. Conseqüentemente, ele deve estar configurado *com software* e *hardware* compatíveis. Por exemplo, as estações com número de patrimônio de 1234 até 1299 são da área de compras, portanto, não precisam possuir os sistemas aplicativos da área de contabilidade ou de recursos humanos.

2.4.8. Formas de proteção

Nos casos em que o usuário se ausentar de seu local de trabalho, recomendamos que ele ative a proteção de tela/bloqueio do teclado. Se por algum motivo o usuário não o fizer, como forma de proteção adicional, as estações de trabalho devem ser configuradas para o bloqueio automático após um período de inatividade.

Como forma de proteger a entrada e, principalmente, a saída de informação da organização, os *drives* de disquete, gravadores de CDs e dispositivos USB devem ter seu uso controlado e autorizado formalmente.

2.4.9. Estações móveis de trabalho

Além das recomendações de segurança citadas para as estações de trabalho, ressaltamos que, estações móveis de trabalho (notebooks/laptops) devem possuir recursos de segurança que impeçam o acesso não autorizado às informações.

2.4.10. Termo de confidencialidade

De forma a obter o comprometimento dos funcionários com as normas, padrões e procedimentos internos da organização, recomenda-se, após a leitura da Política de Segurança, que eles assinem um termo declarando estarem cientes de todo o conteúdo deste importante documento corporativo.

2.5. PROTEÇÃO CONTRA SOFTWARE MALICIOSO

2.5.1. Vírus de computador

É o principal problema de segurança da informação. Como descrito no glossário desta obra, vírus é um programa ou código que se duplica. O vírus pode não fazer nada a não ser propagar-se e deixar o programa infectado funcionar normalmente. Contudo, depois de se propagar silenciosamente por um período, ele começa a exibir mensagens ou pregar peças.

Se um antivírus não possuir uma lista de assinaturas completa, pode ser que ele vasculhe um arquivo contaminado, mas, por não "conhecer" o vírus, deixe-o ileso. A forma como cada programa atualiza essa lista varia de acordo com o fabricante. Esse processo é feito *on-line* e a verificação de novas listas pode ser programada para uma determinada periodicidade.

O uso de software "pirata" está diretamente associado à propagação de vírus em ambientes informatizados.

Devido aos riscos aqui expostos, recomendamos que as políticas possuam, pelo menos, os seguintes procedimentos:

- Uso obrigatório de software antivírus em todos os equipamentos;
- Atualização periódica da lista de vírus e da versão do produto;
- Verificar todo arquivo recebido anexado em e-mail, ou *download* pelo software de antivírus;
- Disponibilizar treinamento adequado que oriente a utilização do software de antivírus para os usuários.

2.5.2. Softwares não autorizados

Uma publicação americana observou que "usuários sempre serão usuários. Ainda que a organização ofereça uma máquina rápida, repleta de memória, certamente ele tentará instalar seus próprios programas". E, por isso, "impedir que usuários acrescentem software não autorizado em

seus computadores de mesa ou *notebooks* se tornou uma preocupação comum entre os gerentes de TI".

Deve-se ressaltar na política, para os usuários, que todos os programas de computador (software) em uso na organização possuem licença de uso oficial e são homologados, sendo proibida a instalação de software de propriedade da organização além da quantidade de licenças adquiridas ou em equipamentos de terceiros.

2.5.3. Procedimentos para acesso à Internet

Embora o acesso à Internet seja praticamente indispensável no local de trabalho, ele pode resultar em perda de produtividade. Na política, devem-se definir regras para proteger os negócios da organização.

O procedimento de uso da Internet deve ser concebido visando padronizar o uso desse recurso. Principalmente, aqueles que tratam da proteção da propriedade intelectual, privacidade das informações e mau uso dos recursos da organização, assédio sexual, racismo, segurança da informação e confidencialidade dos dados da organização e de seus clientes etc.

A Política de Segurança deve especificar que a organização possui os direitos de autoria sobre quaisquer materiais criados internamente por qualquer colaborador.

As páginas da Internet contêm programas que geralmente são inocentes e algumas vezes úteis. Entretanto, existem sites de conteúdo duvidoso e até mesmo malicioso. Ao navegar na Web, é possível identificar o computador na Internet, dizer quais páginas foram acessadas, usar *cookies* para saber o perfil do usuário e instalar *spyware* em computadores, sem o conhecimento do usuário.

Além das atividades maliciosas, os negócios podem ser colocados em uma posição vulnerável por funcionários que se envolvem em atividades ilegais e indesejáveis na Web durante o expediente.

Embora a conexão direta e permanente da rede da organização com a Internet ofereça um grande potencial de benefícios, abre a porta para riscos significativos para os dados e sistemas da organização se não existir uma rígida disciplina de segurança. Qualquer usuário interno da Internet é responsável e pode ser responsabilizado por brechas que intencionalmente afetem a segurança ou a confidencialidade dos dados internos. Não é aconselhado instalar uma conexão permanente sem regras. A organização pode e deve zelar para que isso não aconteça.

Todas as tentativas de conexão devem ser registradas. Os seguintes registros de acesso são o mínimo que a organização deve manter para fins de auditoria:

- Identidade do usuário;
- Data e hora das conexões;
- Endereços IP;
- Protocolos utilizados;
- Quantidade de dados sendo transmitidos e/ou recebidos.

Os usuários que possuem acesso à Internet devem receber treinamento adequado para a explicação das políticas da organização e de suas responsabilidades. Ressaltamos que eles não devem utilizar esse recurso enquanto não passarem pelo treinamento.

2.5.4. Abrangência dos procedimentos de utilização dos recursos da Internet

O procedimento de uso da Internet deve ser submetido à análise do Departamento Jurídico. Devem ser contemplados os seguintes aspectos:

- Se os funcionários terão permissão para navegar na Web para uso pessoal assim como para fins comerciais;
- Se os funcionários poderão usar a Internet para fins particulares e em quais períodos (durante o almoço, depois do expediente etc);
- Se e como a organização efetuará a monitoração do uso da Internet e a qual nível de privacidade os funcionários estão sujeitos;

Acessos não permitidos, determinando os tipos de sites que serão inaceitáveis, como:

- *Download* de conteúdo ofensivo ou preconceituoso;
- Atitude ameaçadora ou violenta;
- Atividades ilegais;
- Solicitações comerciais (não relacionadas ao trabalho);
- Outros aspectos que a organização julgar necessários.

2.5.5. Dicas para uma navegação segura

De forma a promover uma navegação segura, as seguintes recomendações devem ser detalhadas:

- Visitar somente sites confiáveis;
- Nunca navegar em sites a partir de um servidor. Sempre usar uma estação cliente;

- Usar um firewall/roteador para que seja possível filtrar os endereços e bloquear o tráfego de Internet recebido de sites perigosos e enviado para eles;
- Considerar o uso de *software* de filtragem do conteúdo.

2.6. SEGURANÇA LÓGICA

Segundo Fernando Ferreira [9], a segurança em tecnologia da informação pode ser compreendida por dois principais aspectos: segurança lógica e segurança física. A segurança física desempenha um papel tão importante quanto à segurança lógica. Isto porque é a base para a proteção de qualquer investimento feito por uma organização. Investir entre os diferentes aspectos de segurança sem observar suas devidas prioridades pode ocasionar uma perda de todos os recursos investidos, em virtude de uma falha nos sistemas mais vulneráveis [9].

Estatísticas do órgão americano FBI indicam que 72% dos roubos, fraudes, sabotagens e acidentes são causados pelos próprios funcionários de uma determinada organização. Outros 15% ou 20% são causados por terceiros ou consultores que foram formalmente autorizados a acessar as instalações, sistemas e informações da organização. Apenas de 5% a 8% são causados por pessoas externas a organização.

2.6.1. Controle de acesso lógico

Para obtenção de acesso a qualquer ambiente, todos os indivíduos devem ser autenticados e autorizados por algum tipo de sistema. Com a dependência cada vez maior das empresas em relação ao uso do ambiente informatizado, é natural que exista preocupação para implementação de dispositivos de controle de acesso que garantam a segurança de suas instalações mais críticas. E as alternativas disponíveis são diversas como a manual, executado por seguranças, recepcionistas ou funcionários; a automática, com uso de dispositivos específicos para esse fim; e a híbrida, com uso de recursos mistos manuais e automatizados. Cabe ao *Security Officer* analisar a situação e escolher a melhor solução.

Como regra básica, o controle de acesso físico, seja manual ou automatizado, deve ser capaz de distinguir entre a pessoa autorizada e a não autorizada, mediante sua identificação, que deve respeitar pelo menos duas entre três premissas básicas:

- Quem é o indivíduo? Sua identificação e/ou características biométricas.
- O que o indivíduo possui? Utilização de cartões ou chaves.
- O que o indivíduo sabe?

Um sistema de controle de acesso deve ser analisado em relação as seguintes características:

- **Proteção contra ataques forçados**: os controles de segurança devem possuir a mesma resistência que um controle de acesso manual comum, evitando invasões mediante corte de energia força bruta;
- **Atualização do produto**: deve ter capacidade de crescimento ou mudanças e permitir incremento do número de pessoas autorizadas, níveis de privilégios e mudanças nas regras de acesso;
- **Registro dos acessos:** deve ser capaz de registrar todas as tentativas de acesso, dia e qual login foi utilizado para o acesso.

2.6.2. Processo de Logon

O processo de logon é usado para obter acesso aos dados e aplicativos em um sistema informatizado. Normalmente esse processo envolve a utilização de um User ID e uma senha. Para dificultar a tarefa de um invasor, recomenda-se limitar o número de tentativas incorretas de acesso (*logon*), bloqueando a conta do usuário ao alcançar o número limite.

A identificação do usuário, ou User ID, deve ser única, isto é, cada usuário deve ter uma identificação própria. Todos os usuários autorizados devem possuir um código de usuário, quer seja um código de caracteres, cartão inteligente ou outro meio de identificação. Essa unicidade de identificação permite um controle das ações praticadas pelos usuários por meio de *log's* de acesso e atividade dos sistemas operacionais e aplicativos.

Após a identificação do usuário, ocorre sua autenticação, isto é, o sistema confirma se o usuário é ele mesmo. Os sistemas de autenticação são uma combinação de hardware, software e procedimentos que permite o acesso de usuários aos recursos computacionais. Na autenticação, o usuário apresenta algo que ele possui, podendo até envolver a verificação de características físicas. A maioria dos sistemas modernas solicita uma senha (algo que o usuário conhece), ou cartões inteligentes (algo que o usuário possui) ou ainda características físicas, como o formato da mão, da retina ou do rosto, impressão digital e reconhecimento da voz.

2.6.3. Senhas de acesso

Para que os controle de senha funcionem, os usuários devem ter pleno conhecimento das políticas de composição e guarda de senha da organização e serem orientados a segui-las. Funcionários demitidos devem ter suas senhas canceladas.

Recomenda-se que os usuários sejam orientados a escolher senhas mais seguras, evitando o uso de senhas muito curtas ou muito longas, que os obriguem a escrevê-las em um pedaço de papel para memorizá-la. Utilizar a mesma senha em sistemas distintos é uma prática comum, porém vulnerável, pois quando um invasor descobre a senha pela primeira vez, sua atitude é testá-la em outros sistemas. Deve-se evitar a composição de senhas com os seguintes elementos:

- Nome do usuário;
- Igual à conta do usuário;
- Nomes de membros da família ou amigos;
- Nomes de lugares;
- Nome do sistema operacional ou da máquina que está sendo utilizada;
- Datas;
- Números de telefone, cartão de crédito, carteira de identidade ou de outros documentos pessoais;
- Placas ou marcas de carro;
- Letras ou números repetidos;
- Letras seguidas do teclado (asdfg, yuiop, etc);
- Objetos ou locais que podem ser vistos a partir da mesa do usuário;
- Qualquer senha com menos de seis caracteres.

Alguns softwares são capazes de obrigar os usuários a utilizarem senhas complexas. Mas como escolher uma boa senha? São consideradas senhas fortes aquelas que são formadas por letras, números, caracteres especiais e são compostas por mais de seis caracteres. As senhas devem ser trocadas freqüentemente.

Geralmente são consideradas boas senhas aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando mais de seis caracteres. Porém, para ser boa mesmo, a senha tem que ser difícil de ser adivinhada por outra pessoa, mas de fácil memorização, para que não seja necessário anotá-la em algum lugar. Também é conveniente escolher senhas que possam ser digitadas rapidamente, dificultando

que outras pessoas, a uma certa distância ou por cima de seus ombros, possam identificar a seqüência de caracteres. Um método bastante difundido hoje em dia é selecionar uma frase significativa para o usuário e utilizar os primeiros caracteres de cada palavra que a compõe, inserindo símbolos entre eles.

2.6.4. Sistemas biométricos

Segundo José Pinheiro, a biometria pode ser definida como a ciência da aplicação de métodos de estatística quantitativa a fatos biológicos, ou seja, é o ramo da ciência que se ocupa da medida dos seres vivos (do grego bio = vida e métron = medida). Resumindo, a biometria é a autenticação / identificação de um indivíduo pelas suas características biológicas e comportamentais [13].

Os sistemas biométricos são uma evolução natural dos sistemas manuais de reconhecimento, como a análise grafológica de assinaturas, análise de impressões digitais e o reconhecimento da voz.

A biometria pode ser utilizada em um sistema de informação para resolver dois problemas importantes: a identificação e o acesso de usuários à rede de computadores.

Os sistemas biométricos utilizados na segurança em uma rede de computadores buscam verificar a identidade de um indivíduo (identificação) através das características únicas inerentes a essa pessoa por meio de processos automatizados. Essas características podem ser físicas (olhos, mão, etc) e / ou comportamental (modo como assina um documento, por exemplo).

No controle de acesso, os sistemas biométricos permitem que um indivíduo possa ser autenticado na rede sem a necessidade de uma senha ou outro dispositivo físico (crachá, cartão eletrônico, etc), ou ainda (e mais usualmente) em combinação com estes. Os sistemas biométricos têm algumas vantagens em relação aos sistemas tradicionais, na medida em que a informação necessária para permitir o acesso não é perdida ou susceptível de apropriação ilícita. Por outro lado, a pessoa não necessita de recordar números, códigos ou qualquer outra chave de identificação.

A autenticação biométrica envolve duas fases: registro no sistema (coleta de dados) e reconhecimento da característica biométrica. Para isso é necessário primeiramente que todos os usuários sejam cadastrados através de um dispositivo de entrada de dados, geralmente um

scanner, microfone, leitor óptico ou outro meio eletrônico, para colher a representação digital que será usada na verificação do indivíduo.

O cadastramento envolve o indivíduo que irá fornecer uma amostra de sua característica biométrica, sendo que essa característica-chave será usada pelo sistema para gerar um modelo biométrico. A amostra é convertida para um algoritmo matemático que então é criptografado. Cada vez que o usuário requerer um acesso ao sistema, uma verificação / autenticação será realizada e a amostra da característica particular do indivíduo será comparada com o modelo biométrico armazenado no banco de dados.

Algumas das principais características dos sistemas biométricos:

- Impressões digitais**:** são características únicas e consistentes. Nos sistemas biométricos que utilizam esta opção, são armazenados de 40 a 60 pontos para verificar uma identidade.O sistema compara a impressão lida com sua base de dados de impressões digitais de pessoas autorizadas.

- Voz: os sistemas de reconhecimento de voz são usados para controle de acesso, porém não são tão confiáveis, em função dos erros causados por ruídos no ambiente e problemas na garganta ou nas cordas vocais das pessoas a ele submetidas.

- Geometria da mão: também é usada em sistemas de controle de acesso, porém essa característica pode ser alterada por aumento ou diminuição de peso ou artrite.

- Configuração da íris e da retina: esses sistemas se propõem a efetuar uma identificação mais confiável do que as impressões digitais. Entretanto são sistemas evasivos, pois direcionam feixes de luz para os olhos das pessoas.

- Reconhecimento facial por meio de termograma: o termograma facial é uma imagem retirada com uma câmara infravermelha que mostra padrões térmicos de uma face. Essa imagem é única e, combinada com algoritmos sofisticados de comparação de diferentes níveis de temperatura distribuídos pela face, constitui-se em técnica não evasiva, altamente confiável, não sendo afetada por alterações de saúde, idade ou temperatura do corpo. São armazenados ao todo 19.000 pontos de identificação, podendo distinguir gêmeos idênticos, mesmo no escuro. Pesquisas estão sendo feitas na área fins baratear seus custos.

2.6.5. Controle de Acesso à Rede

Os acessos internos e externos aos serviços de rede devem ser controlados e liberados de acordo com a necessidade de cada usuário, dependendo do tipo de acesso, caminho utilizado, criticidade das informações, recursos a serem disponibilizados, entre outros.

Os pontos de rede devem ser protegidos (com autenticação, por exemplo) para impedir a conexão de estações não autorizadas.

O acesso às portas de diagnóstico dos equipamentos (*switches, routers* , etc.) deve ser seguramente controlado.

É preciso segmentar as redes logicamente, isolando os servidores de missão crítica ou sensíveis ao negócio da organização (uma rede para os servidores e outra para as estações), cada uma das quais protegidas por um perímetro de segurança definido. Tal perímetro pode ser implementado com a instalação de um *gateway* seguro entre as duas redes que serão interligadas para controlar o acesso e o fluxo de informações entre os dois domínios. Este *gateway* deve ser configurado para filtrar o tráfego entre estes dois domínios bloqueando acessos não autorizados de acordo com a política de controle de acesso da organização. Um exemplo deste tipo de *gateway* é freqüentemente referenciado como *firewall* .

As funcionalidades de segurança do sistema operacional, quando existentes, devem ser usadas para restringir o acesso aos recursos computacionais. Além disso, convém que os acessos aos serviços de informação sejam realizados através de um processo seguro de entrada no sistema (*logon*).

Terminais inativos em locais de alto risco, por exemplo, em áreas públicas ou externas (fora dos limites do gerenciamento de segurança da organização), ou servindo a sistemas de alto risco, devem contar com sistema de desligamento automático após um período predeterminado de inatividade, de forma a prevenir contra o acesso de pessoas não autorizadas.

A mesma preocupação deve ser necessária com relação à computação móvel (*notebooks, palmtops, laptops* , telefones celulares, etc) e acessos remotos, adotando-se, por exemplo, recursos de autenticação forte e criptografia.

2.6.6. Combate a ataques e invasões

Destinados a suprir a infra-estrutura tecnológica com dispositivos de software e hardware de proteção, controle de acesso e conseqüente combate a ataques e invasões, esta família de mecanismos tem papel importante no modelo de gestão de segurança, à medida que as conexões eletrônicas e tentativas de acesso indevido crescem exponencialmente. Nesta categoria, existem dispositivos destinados ao monitoramento, filtragem e registro de acessos lógicos, bem como dispositivos voltados para a segmentação de perímetros, identificação e tratamento de tentativas de ataque.

Firewall

Velho conhecido dos ambientes de rede, este dispositivo, que pode assumir a forma de um software e também incorporar um hardware especializado, tem o papel de realizar análises do fluxo de pacotes de dados, filtragens e registros dentro de uma estrutura de rede. Como o próprio nome diz, ele representa uma parede de fogo que executa comandos de filtragem previamente especificados com base nas necessidades de compartilhamento, acesso e proteção requeridos pela rede e pelas informações disponíveis através dela.

Buscando um modelo didático, podemos compará-lo ao tradicional filtro de água doméstico que, a princípio, é formado por um compartimento vazio por onde passa a água supostamente poluída, e por um elemento ou vela contendo camadas de filtragem formadas por diversos materiais. Ao passar por este compartimento, já com o elemento de filtragem, as impurezas da água são retidas pelas diversas camadas do elemento. Desta forma, o filtro poderá ser considerado eficiente se conseguir reter todas as impurezas e permitir a passagem de todos os demais componentes benéficos à saúde, como sais minerais etc. *O firewall* se assemelha ao filtro por também necessitar da especificação de camadas de filtragem específicas para cada empresa e situação, com o propósito de impedir acessos indevidos que ocorram de dentro ou de fora da rede, registrando essas ocorrências e, principalmente, permitindo o tráfego normal de pacotes de dados legítimos. Por ser baseado na análise binária de parâmetros definidos no filtro, *o firewall* age sempre da mesma maneira e sem considerar variáveis externas que possam modificar as situações; portanto, a eficiência de proteção desse dispositivo está ligada diretamente à adequada especificação e manutenção das regras de filtragem.

É importante lembrar que surgiu uma categoria *de firewall* destinada ao usuário final, chamada *personal firewall*, com o propósito de estender a segurança e complementar à

proteção. Obviamente são recursos de software com baixa performance, mas adequadamente proporcionais, na maioria das situações, ao volume de dados trafegados em uma conexão desse gênero.

Detector de Intrusos

Normalmente chamado pela sigla em inglês IDS, o detector de intrusos é um dispositivo complementar ao *firewall* que agrega maior inteligência ao processo de combate a ataques e invasões. Diferente do *firewall,* o IDS é orientado por uma base de dados dinâmica contendo informações sobre comportamentos suspeitos de pacotes de dados e assinaturas de ataques. É uma verdadeira enciclopédia de ameaças consultada a todo o momento para que o dispositivo possa transcender a análise binária de situações e avaliar a probabilidade de um acesso ser um conhecido tipo de ataque ou uma nova técnica de invasão. Ainda não estamos falando de inteligência artificial; afinal, a ferramenta não aprende com as próprias experiências e não gera conclusões de forma autônoma, mas o dispositivo demonstra seu potencial como sinalizador de situações que fujam à normalidade. É importante ressaltar que, por possuir um grau de inferência sobre possíveis situações de risco, o detector de intrusos é responsável por muitos falso-positivos, ou seja, por sinalizar situações aparentemente estranhas, mas que são legítimas. Por conta disso, dependendo do ambiente protegido e do grau de tolerância à indisponibilidade de acesso, não é conveniente deixar que o IDS aja sozinho, mas que atue como um instrumento de sinalização para que os técnicos possam avaliar a situação e, então, decidir pelo bloqueio ou pela permissão.

Existem dispositivos que, apesar de terem sido desenvolvidos originalmente para outros fins, incorporaram, com o passar do tempo, recursos que auxiliam e, muitas vezes, reforçam atividades de bloqueio e combate a ataques. O roteado com filtro, por exemplo, incorpora parte das funcionalidades de *um firewall,* e o *switch,* naturalmente destinado à melhoria de performance e gerenciamento das redes, tem grande aplicabilidade na segmentação lógica da mesma, reduzindo a eficiência de tentativas de ataque que monitoram o meio, grampeando-o, a fim de capturar informações relevantes. Da mesma forma, o *proxy,* software com o propósito de aumentar a performance do acesso ao serviço Web da Internet através da gerência de conteúdo como se fosse uma memória *cache,* tem o potencial de filtrar e registrar acessos proibidos que sinalizam o descumprimento das normas da política de segurança.

2.6.7. Privacidade das comunicações

É inevitável falar de criptografia quando o assunto é privacidade das comunicações. A criptografia é uma ciência que estuda os princípios, meios e métodos para proteger a confidencialidade das informações através da codificação ou processo de cifração e que permite a restauração da informação original através do processo de decifração. Largamente aplicada na comunicação de dados, esta ciência se utiliza de algoritmos matemáticos e da criptoanálise, para conferir maior ou menor proteção de acordo com sua complexidade e estrutura de desenvolvimento. Quando vemos *softwares* de criptografia de mensagem ou por exemplo, aplicações que adotam criptografia, estamos diante de situações em que a ciência foi empregada e materializada em forma de programas de computador. Existem duas técnicas principais de criptografia.

1. **Simétrica ou de chave privada**

Técnica criptográfica que utiliza uma única senha, ou chave, para cifrar informações na origem e decifrá-las no destino. Apesar de sua excelente performance, entre outras coisas pela existência de uma única chave que confere velocidade aos processos matemáticos de cálculo, este método tem uma vulnerabilidade nativa presente no processo de envio ou compartilhamento da chave simétrica com o destinatário. Usando um exemplo hipotético em que se quer enviar uma mensagem criptografada do usuário A para o usuário B, o primeiro passo seria criar uma chave simétrica e enviar uma cópia da mesma ao destinatário para que ele pudesse decriptografar a mensagem após recebê-la. O risco ocorre justamente no momento do envio da cópia da chave ao destinatário por não ter sido adotado nenhum processo de proteção. Se, exatamente neste momento frágil, apesar da pequena janela de tempo da operação, a confidencialidade da chave for quebrada, todo o processo de criptografia fica comprometido; afinal, qualquer um que conheça a chave simétrica poderá decriptografar a mensagem interceptada. Um dos algoritmos de chave simétrica mais utilizados no mundo é o DES - *Data Encryption Standard,* criado em 1977, com chave criptográfica de 56 bits, além do 3DES, RC2, RC4 e *Blowfish.* O tamanho da chave criptográfica está diretamente ligada ao nível de segurança do algoritmo devido ao aumento exponencial de possibilidades e tentativas necessárias para "quebrar", ou seja, para descobrir a chave certa que decifre a proteção.

2. Assimétrica ou de chave pública

Técnica criptográfica que utiliza um par de chaves para cada um dos interlocutores, mais especificamente uma chave privada e outra pública para o remetente, e o destinatário. Desta forma, com a criptografia assimétrica criada em 1976 por Diffie e Hellman, os interlocutores não precisam mais compartilhar uma chave única e secreta. Baseado no conceito de que para decifrar a criptografia é necessário possuir as duas chaves matematicamente relacionadas, pública e privada, o remetente só precisa da chave pública do destinatário para garantir a confidencialidade da mensagem e para permitir que o destinatário consiga decifrar a mensagem.

Como o próprio nome diz, a chave privada pertence exclusivamente ao seu proprietário e deve ser mantida em segredo. A pública, por sua vez, pode e deve ser compartilhada e estar disponível a qualquer interessado em enviar uma mensagem a você de forma criptografada. Este técnica ainda reserva recursos complementares, como a assinatura digital, obtida pela utilização da chave privada para fazer uma "marca binária" na mensagem, sinalizando ter sido escrita e enviada pelo proprietário da própria. O certificado digital é um instrumento eletrônico que atesta a veracidade da chave pública do usuário, conferindo autenticidade ao documento assinado digitalmente.

Não podemos nos esquecer, também, da função HASH, que confere a possibilidade de verificar a integridade de uma mensagem a partir da comparação, no destino, do resultado obtido pela aplicação da função. Quando os resultados obtidos pela função na origem não coincidem com os resultados obtidos no destino, tem-se a indicação de que a mensagem sofreu qualquer tipo de alteração, mesmo que muito pequena.

Aparentemente esta técnica se mostra perfeita, se não fosse pelo fato de possuir baixa performance, chegando a consumir centenas ou milhares de vezes mais tempo para ser processada se compararmos com a técnica simétrica.

Devido aos problemas presentes em ambas as técnicas, foi encontrada uma solução híbrida a partir da união de técnicas que permitiu usufruir da performance da simétrica e da segurança e funções satélites de assinatura digital e validação de integridade proporcionadas pela técnica assimétrica. De posse do par de chaves pública e privada, o remetente gera a chave simétrica e insere um cópia em uma nova mensagem, método este que se convencionou chamar de envelopamento, criptografando-a com a chave pública do destinatário. Este por sua vez, ao receber a mensagem confidencial, lança mão de sua

chave privada para decifrá-la, obtendo acesso à cópia da chave simétrica. A partir deste momento, em que ambos estão de posse da chave simétrica enviada e recebida em segurança, o processo de comunicação criptografada pode ser reiniciado adotando esta mesma chave simétrica que irá conferir a velocidade necessária para viabilizar a troca de informações.

Virtual Private Network

Esta solução, comumente chamada pelo acrônimo VPN, é fruto da aplicação de criptografia entre dois pontos distintos através de uma rede pública ou de propriedade de terceiros. O resultado da adoção de criptografia é a criação de um túnel seguro que garante a confidencialidade das informações sem, no entanto, absorver os riscos nativos de uma rede que transcende seus limites de controle. Desta forma, a empresa passa a ter uma rede virtual privada, ou seja, a tecnologia viabiliza o uso de uma rede nativamente insegura como se parte dela fosse privada pela segurança agregada pelo tunelamento. Para cumprir o papel de extensão de sua rede corporativa, a VPN precisa garantir o mínimo de performance a fim de viabilizar conexões com filiais e parceiros, usufruindo, assim, dos benefícios de capilaridade e redundância que a Internet, por exemplo, oferece. Assim, são implementadas por software e hardware especializados e capazes de processar a codificação e a decodificação dos pacotes de dados com extrema velocidade e competência.

É importante lembrar que surgiu uma categoria de *virtual private network* destinada ao usuário final, chamada *personal VPN*, com o propósito de permitir conexões remotas seguras. Obviamente são recursos de software com baixa performance, mas adequadamente proporcionais, na maioria das situações, ao volume de dados trafegados em uma conexão desse gênero.

Public Key Infrastruture

É possível notar a grande aplicabilidade do certificado digital em processos de autenticação e criptografia, seja na publicação de informações, acessos a ambientes físicos, aplicações e equipamentos, envio de mensagens eletrônicas, redes virtuais privadas, ou na troca eletrônica de informações em geral. Sua versatilidade e potencial de crescimento trazem à tona um potencial problema: o gerenciamento do processo de emissão, revogação, guarda e distribuição; afinal, para que os documentos e processos possam assumir a credibilidade do agente ou usuário do dispositivo, a mesma dever ter sido herdada do processo de gerenciamento do dispositivo. Por conta dessa necessidade, a tecnologia PKI, ou Infra-

estrutura de Chaves Públicas em português, reúne recursos de software e serviços para suportar a montagem de um processo de gestão de certificados. Buscando um exemplo que privilegie a didática, podemos fazer uma analogia com os cartórios tradicionais. Para que a compra de um bem seja concretizada, muitos documentos precisam ser autenticados por uma estrutura que tenha fé pública ou, no mínimo, confiança das partes envolvidas na transação. Este processo requer a presença física para identificação das partes através de documentos, comprovação visual da autenticidade dos documentos originais para, então, estender a originalidade às cópias.

De forma similar, o processo de certificação digital implementado com a infra-estrutura de PKI requer a identificação prévia das partes para, só então, emitir o instrumento digital. Além disso, essa mesma estrutura tem de estar orientada por uma política específica e ser capaz de reemitir, revogar, distribuir e, principalmente, manter sob altos critérios de confidencialidade, integridade e disponibilidade o segredo do processo: a chave privada e seus critérios de concepção.

A percepção da importância técnica do assunto e, principalmente, dos fatores legais que envolvem a responsabilização de pessoas e empresas pela relação eletrônica de informações reconhecidas como legítimas, já chegou ao setor público. O interesse do governo é orientar e subsidiar uma base comum de construção de infra-estruturas de chaves pública para, no primeiro momento, garantir o reconhecimento mútuo das empresas e a administração pública federal dentro do país e, em um segundo momento, viabilizar o reconhecimento por outras estruturas internacionais integradas, que fomentarão o comércio eletrônico, as relações governamentais e empresariais. O reflexo desse movimento se materializou em agosto de 2001, através da medida provisória MP-2002-2, que institui uma infra-estrutura de chaves públicas do Brasil, ou ICP-Brasil, cuja definição vem a ser “um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.”

2.7. SEGURANÇA FÍSICA E DO AMBIENTE

Os sistemas de segurança devem ser implementados para garantir que em todos os locais da organização o acesso seja realizado apenas por profissionais autorizados. Quanto maior for a sensibilidade do local, maiores serão os investimentos em recursos de segurança para serem capazes de impedir o acesso não autorizado.

De acordo com o Portal do Governo do Estado de São Paulo, “Os recursos e instalações de processamento de informações críticas ou sensíveis ao negócio devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.”

A proteção física pode ser alcançada através da criação de diversas barreiras em torno da propriedade física do negócio e de suas instalações de processamento da informação. Cada barreira estabelece um perímetro de segurança, contribuindo para o aumento da proteção total fornecida. A proteção fornecida deve ser proporcional aos riscos identificados, sendo necessário a implementação de controles de entrada apropriados para assegurar que apenas pessoas autorizadas tenham acesso as informações.

As paredes externas do local devem ser sólidas e todas as portas externas protegidas de forma apropriada contra acessos não autorizados, como, por exemplo, mecanismos de controle, travas, alarmes, etc.

Deve-se levar em consideração as possibilidades de dano causado por fogo, inundação, explosão, manifestações civis e outras formas de desastres naturais ou causados pelo homem.

Ainda com relação aos aspectos citados, recomenda-se o seguinte:

- Isolar as instalações críticas do acesso público, mantendo os servidores em local reservado com acesso controlado;
- Manter um controle restrito de entrada e saída de pessoas no recinto, utilizando sistemas de controle de entrada através de códigos de acesso, crachás autorizados entre outras tecnologias disponíveis no mercado;
- Jamais permitir a instalação de equipamentos que permitam a duplicação de informações no mesmo ambiente em que as mesmas se encontram ou dentro de áreas de segurança, como por exemplo, fotocopiadoras, *scanners*, unidades de gravação de CDs e máquinas de fax, para evitar vazamento de informação;
- Proibir a entrada de filmadoras e câmeras fotográficas nestes ambientes;

Portas e janelas devem ser mantidas fechadas quando não utilizadas e, sempre que possível, implementar um sistema de alarme.

2.7.1. Acesso de funcionários e terceiros às dependências da organização

As políticas devem especificar que todos os funcionários da organização somente terão acesso liberado às dependências da organização se portarem a identificação funcional pessoal. Já para as áreas restritas, os acessos deverão ser previamente solicitados e autorizados, por meio de procedimentos formais criados para tal atividade.

O acesso de prestadores de serviço, contratos para as consultorias, manutenções e/ou quaisquer outros serviços, deverão obter autorização formal antecipada para o acesso às dependências.

A Norma NBR/ISO 17799 [12] sugere diversos requisitos de segurança de terceiros dentro da organização, principalmente no tocante a contratos, entre os quais destacamos a necessidade de serem incluídos nos contratos os requisitos de segurança física.

2.7.2. Controle de acesso físico

O controle de acesso físico é toda e qualquer aplicação de procedimentos ou uso de equipamentos com o objetivo de proteger ambientes, equipamentos ou informações cujo acesso deve ser restrito. Esse tipo de controle envolve o uso de chaves, trancas, guardas, crachás, cercas, alarmes, vídeo, *smart cards*, biometria e etc, além da aplicação de normas e procedimentos utilizados pela organização para esse fim.

A política e o investimento, no controle de acesso físico adotada pela organização, estarão diretamente ligados à importância de seus ativos, observando sempre a relação custo/benefício. Uma política de controle de acesso físico eficaz dependerá muito mais da gestão dos modelos de segurança do que apenas do uso de tecnologia. Nesse sentido, é fundamental a análise do perfil de cada organização, para a definição de uma política de controle de acesso físico que atenda suas necessidades. Quanto maior o investimento em prevenção menor será o prejuízo em caso de eventos. O investimento em questão não se refere apenas ao uso de tecnologia de ponta, mas a forma como a empresa conscientiza seu quadro de funcionários.

Tipos de controles de acesso físico, bem como suas características:

- Grades, muros e portas: determinam um limite, objetivando inibir a presença de curiosos. As grades devem ter alarmes ou estarem sob vigilância de guardas ou monitores de TV;

- Guardas: posicionados na entrada de instalações consideradas estratégicas, para controlar o acesso e permitir a entrada somente de pessoal autorizado. A ação dos guardas também é bastante eficaz na inspeção de pacotes e outros itens de mão na entrada e na saída. A eficiência do trabalho dos guardas será otimizada com a aplicação de tecnologia, como a instalação de alarmes, câmeras e outros dispositivos;

- Crachás: funcionários e visitantes devem ser obrigados a usá-los para obterem acesso. Esse sistema não envolve necessariamente a aplicação de tecnologia, mas o cumprimento das políticas e procedimentos internos. Recomenda-se que os crachás contenham poucas informações. Assinaturas e detalhes por escrito sobre privilégios de acesso devem ser evitados. A identificação pode ser feita por códigos ou cores e o número de série dos crachás deve ser único; Sistemas com portas duplas: podem ser usadas para forçar as pessoas a identificarem-se junto a um guarda, que se posiciona na entrada da segunda porta. Esse tipo de sistema é ideal para prevenir a entrada de intrusos que têm acesso a áreas restritas seguindo pessoas autorizadas; Controle de acesso biométrico: este é o método de identificação mais sofisticado utilizado atualmente. Biometria usada para a identificação inclui a impressão digital, leitura da palma da mão, padrões de voz, escaneamento de retinas, entre outras. Como o controle biométrico não pode ser compartilhado, perdido, roubado, ou esquecido, é considerado altamente eficaz.

2.7.3. Controles ambientais

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

Os equipamentos devem ser instalados e protegidos para reduzir o risco de ameaças ambientais, perigos e oportunidades de acesso não autorizado. Recomenda-se que os seguintes itens sejam considerados:

- As instalações de processamento e armazenamento de informação que tratam as informações sensíveis devem ser projetadas para reduzir riscos de espionagem de informações durante o seu uso;

- Os itens que necessitam de proteção especial devem ser isolados para reduzir o nível geral de proteção exigida;

- Adotar controles de forma a minimizar ameaças potenciais, incluindo:
    - Fogo;
    - Explosivos;
    - Fumaça;
    - Água;
    - Poeira;
    - Vibração;
    - Interferência no fornecimento elétrico;

- Aspectos ambientais devem ser monitorados para evitar condições que possam afetar de maneira adversa a operação das instalações de processamento da informação;

- Utilização de métodos de proteção especial, como capas para teclados, seja considerada para equipamentos em ambiente industrial;

- Também deve ser considerado o impacto de um desastre que possa ocorrer nas proximidades da instalação, como por exemplo, um incêndio em um prédio vizinho, vazamentos de água no telhado ou em andares abaixo do nível do chão ou explosões na rua.

2.7.4. Segurança física de computadores pessoais

Quando se utilizam recursos da computação móvel, por exemplo, *notebooks*, *paimtops*, laptops e telefones celulares, devem ser tomados cuidados especiais para assegurar que a informação da organização não seja comprometida. Uma política formal deve ser adotada, levando-se em conta os riscos de trabalhar com tais recursos móveis, particularmente em ambientes desprotegidos.

Devem ser tomadas certas precauções ao se utilizarem os recursos de computação móvel em locais públicos, salas de reuniões e outras áreas desprotegidas fora dos limites da organização. Devem ser estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nestes recursos (criptografia).

É importante que, quando tais recursos forem utilizados em locais públicos, seja tomado cuidado para evitar o risco de captação por pessoas não autorizadas. Também devem ser estabelecidos procedimentos contra software pirata/malicioso e vírus, mantendo-os sempre atualizados.

Adicionalmente, os recursos de computação móvel também devem ser protegidos fisicamente contra roubo, especialmente quando deixados, por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião. Os equipamentos que contêm informações críticas nunca devem ser deixados sem observação e, quando possível, devem ser fisicamente trancados ou que travas especiais sejam utilizadas de forma a manter o equipamento seguro.

2.7.5. Investimentos em segurança física e ambiental

O primeiro passo a ser tomado para investir em segurança física deve ser a realização de uma análise dos riscos e vulnerabilidades físicas que a organização possa estar exposta. Esta análise deve ser feita, preferencialmente, por especialistas no assunto e, se possível, externos à organização, para que não haja conflito ou compromisso com relação a projetos realizados com ou sem sucesso. Existem diversas ferramentas para auxiliara análise dos impactos nos negócios, em virtude de eventos ou sinistros aos quais a empresa possa estar exposta.

A análise de riscos deverá retratar a real situação da organização quanto aos aspectos de segurança física. Os resultados devem ser encarados como uma ferramenta para auxiliar a organização a melhorar ou manter seu nível de segurança física. Muitas vezes as organizações não utilizam a análise de riscos como uma ferramenta, em razão de não quererem mudar o que já foi feito ou por acreditarem que ao fazê-lo estarão assumindo suas deficiências e erros passados.

Num cenário de mudanças constantes em Tecnologia da Informação, onde sistemas devem ser flexíveis e preparados para evoluções e alterações, a segurança da informação também deve ser capaz de acompanhar estas mudanças. Desta forma, a segurança física, apesar de seu conceito tradicional estar ligado à solidez e estabilidade, precisa ser flexível e capaz de absorver as diferentes tecnologias que surgem ao longo do tempo. As organizações precisam estar constantemente revisando e reorganizando seus componentes e processos de segurança física.

O segundo passo, após uma análise de riscos físicos, deve ser o levantamento das necessidades de componentes e processos de segurança física. Nesta etapa, deve ser envolvido um comitê responsável pela continuidade dos negócios da organização e/ou uma empresa contratada para a elaboração do plano, em razão de envolver assuntos correlacionados de segurança lógica e técnica. Nesta fase, decide-se sobre todos os recursos a serem

disponibilizados como equipamentos de monitoração, energia, climatização, ambientes de segurança para os equipamentos críticos, política de segurança de acesso físico às informações e ambientes distintos da organização, dentre os diversos componentes e processos que devem ser envolvidos num projeto de segurança física.

A última fase envolve a implementação do plano de segurança física, que faz parte de um projeto maior de continuidade de negócios. Após realizar os investimentos e implementar o plano, a organização deverá revê-lo e modificá-lo periodicamente, se necessário.

2.8. CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DA INFORMAÇÃO

A classificação das informações é necessária para seu melhor gerenciamento. Se implementada corretamente, a classificação reduz drasticamente o custo com recursos para proteger as informações e ajuda na implementação de controles onde realmente são necessários.

Segundo Fernando Ferreira [9], o processo de classificação aumenta a confiabilidade dos dados garantindo sua confidencialidade, integridade e disponibilidade. Adicionalmente, boas práticas de segurança são aprimoradas como resultado da correta classificação e destino dos recursos identificados. A política de segurança da informação corporativa deve ser a base fundamental para este processo de classificação, bem como o primeiro passo para obtenção do comprometimento da alta cúpula da organização.

O projeto e o conceito de classificação dos ativos de informação dependem da Política de Segurança das Informações corporativa, implementada e formalmente divulgada a todos os funcionários, terceiros, colaboradores ou qualquer indivíduo que possua acesso a um tipo de informação, declarando que os dados são um ativo da organização e devem ser protegidos. Neste mesmo documento, deve-se citar que as informações serão classificadas com base em seu valor, risco de sua perda ou modificação e exigências legais. Esta política fornece ao *Security Officer* as bases necessárias para iniciar um projeto, bem como exigir o comprometimento da Alta Administração.

Poderão ser utilizados os seguintes critérios para auxiliar a classificação:

- Informações para auditoria: quanto custa, onde estão localizadas e quais os controles estão em vigor para minimizar o risco de divulgação, alterações não autorizadas?

- A segregação de funções é necessária: Sim ou Não? Caso afirma de que forma é realizada/controlada?
- São utilizados mecanismos de criptografia?
- Como é realizado e administrado o procedimento de controle de acesso?
- Os procedimentos e controles sobre os *backups* estão documentados?
- Qual a localização da documentação?

Adicionalmente, os controles descritos abaixo são necessários para completar a estrutura de controles sobre as informações, mas precauções dever tomadas para assegurar que todos os controles de segurança implementados são adequados para cada tipo de classificação da informação:

- Utilizar controles recomendados pela auditoria;
- Desenvolver e realizar planos de teste;
- Segregar todas as funções;
- Procedimentos formais para o gerenciamento de mudanças.

Após a classificação das aplicações e informações, deve-se elaborar e implementar procedimentos para monitoramento contínuo. Geralmente, o departamento de auditoria da organização fica encarregado de liderar e iniciar esta atividades para garantir a conformidade com a política organizacional. O *Security Officer*, em conjunto com os proprietários da informação, deve, periodicamente, revisar as informações classificadas para assegurar que elas estão adequadamente classificadas. Adicionalmente, os privilégios e direitos de acesso dos usuários devem ser revisados para assegurar que estão de acordo com as necessidades de cada um.

Uma vez que os critérios de classificação estão adequadamente definidos e implementados, a equipe deverá determinar a classificação que será utilizada e os controles de segurança adequados. Fatores especiais, incluindo exigências legais, devem ser consideradas no momento de estabelecer a classificação.

Muitas classificações não são aconselhadas, pois poderão gerar confusões para os proprietários das informações ou encontrar algum tipo de resistência para sua implementação. A equipe não deve permitir que as áreas de negócio utilizem classificações diferentes daquelas especificadas nas políticas da organização.

Cada classificação deve ser de fácil compreensão e claramente descrita para demonstrar a diferenciação entre cada uma delas. Segue abaixo exemplo utilizado por muitas organizações:

Classe 1: pública/informação não classificada

Informações que, se forem divulgadas fora da organização, não trarão impactos aos negócios. A integridade dos dados não é vital. Exemplo: testes de sistemas ou serviços sem dados confidenciais, brochuras e folders da organização.

Classe 2: informação interna

O acesso externo às informações deve ser evitado. Entretanto, se estes dados tornarem-se públicos, as conseqüências não são críticas. A integridade dos dados é importante, mas não é vital. Exemplo: agendas de telefones e ramais, grupos de desenvolvimento de sistemas aplicativos onde os dados utilizados são fictícios.

Classe 3: informação confidencial

As informações desta classe devem ser confidenciais dentro da organização e protegidos de acesso externo. Se alguns destes dados forem acessados por pessoas não autorizadas, as operações da organização podem ser comprometidas, causando perdas financeiras e perda de competitividade. A integridade dos dados é vital. Exemplos: salários, dados pessoais, dados de clientes, senhas e informações sobre as vulnerabilidades da organização.

Classe 4: informação secreta

O acesso interno ou externo não autorizado a estas informações é extremamente crítico para a organização. A integridade dos dados é vital. O número de pessoas com acesso as informações deve ser muito pequeno, bem como regras restritas para sua utilização. Exemplos: informações de votação secreta ou contratos confidenciais.

Segundo Profª. Vera Paucker Harger [14], os ativos da organização devem ser inventariados, classificados de acordo com o grau de confidencialidade, disponibilidade e integridade e haver um proprietário com a responsabilidade da manutenção dos controles apropriados, voltados a garantir a segurança dos ativos em questão. Ativos são todos os serviços, informações, sistemas computadorizados e equipamentos da organização. As informações necessitam ser classificadas e rotuladas, de acordo com o grau de confidencialidade exigido pelos negócios da Companhia, para que recebam um nível apropriado de proteção. Desta forma, também necessitam ser inventariadas e receber um

proprietário com a incumbência de protegê-las. Adicionalmente, cuidados com o manuseio das informações devem ser endereçados de acordo com seus rótulos .

2.9. ENGENHARIA SOCIAL

Há uma frase de Ællen Frisch [15] que diz: “Segurança tem início e termina com as pessoas”. Muitos executivos pensam que é suficiente a implementação de regras, regulamentos, políticas, normas, bem como o uso de programas de proteção da informação. Estas são ações importantes, contudo são parte da solução. É essencial que haja a conscientização das pessoas da organização, sejam elas funcionários, prestadores de serviços, executivos e acionistas. Infelizmente a informação não é considerada como fonte preciosa de posse particular. Ou seja, como objeto preponderantemente valioso que cada funcionário carrega consigo, desde o momento em que se instala na empresa até o presente momento. Funcionários despreparados podem ser alvos fáceis da técnica denominada Engenharia Social.

Mas o que vem a ser Engenharia Social? Emerson Alecrim [16] a define como sendo “qualquer método usado para enganação ou exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes.” Ou, segundo um dos maiores especialistas na arte da Engenharia Social, Kevin Mitnick [17]: “É um termo diferente para definir o uso da persuasão para influenciar as pessoas a concordar com um pedido”.

Em geral, o Engenheiro Social tem o perfil do tipo de pessoal agradável, simpática, educada e carismática. Além disso, é criativo, flexível e dinâmico, possuindo uma conversa bastante envolvente. Ele utiliza várias ferramentas para a prática da engenharia social, dentre elas têm-se:

- **Telefone ou VoIP (voz sobre IP)**: passam-se por alguém que não é,
- **Internet**: utilizam sites que fornecem id e *passwords*, sites clonados ou via FTP, Orkut, registro.br, Google, dentre outros.
- **Intranet (acesso remoto)**: captura o micro de determinado usuário da rede e se passa por alguém que na verdade não é. Pode se tratar de funcionário insatisfeito, que constitui uma das maiores ameaças existentes.
- **E-mail**: emails falsos (*Fakemails*), *phishing* scam.
- **Pessoalmente**: o engenheiro social faz-se passar por alguém que na verdade ele não é. Utiliza a persuasão e como um artista de teatro, adota toda uma encenação, a fim de manipular a vítima de forma bastante convincente no que diz.

- **Chats (bate papo)**: Utilizam softwares de canais de bate-papo, tais como Messenger, ICQ, IRC para obter informações valiosas, passando-se por alguém que na verdade não é.

- **Fax:** praticando os mesmos princípios do *email*, o engenheiro social envia pedidos de requisição, formulários de preenchimento, dentre outros, para posterior retorno do que se deseja obter.

- **Cartas/correspondências:** utilizado principalmente para enganar pessoas mais velhas e principalmente aquelas que têm certa resistência à tecnologia. Daí o engenheiro social elabora cartas – documentos com logomarcas e tudo mais, dando a impressão de que se trata realmente da origem.

- **Sypware:** software espião usado para monitorar de modo oculto as atividades do computador alvo.

- **Mergulho no lixo ("Dumpster diving"):** muitas informações valiosas são jogadas no lixo diariamente sem que o documento passe por um triturador.

- **Surfar sobre os ombros:** é o ato de observar se uma pessoa digitando no teclado do computador para descobrir e roubar sua senha ou outras informações de usuário, em geral em locais públicos.

- **P2P (Peer-to-Peer):** tecnologia empregada para estabelecer uma espécie de rede de computadores virtual onde cada estação possui capacidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, no qual alguns computadores são dedicados a servirem dados a outros. Aparentemente mal empregado, o termo *Peer-to-Peer*, quando usado para aplicações como o *Napster*, ressaltam a importância do papel exercido pelos nós da rede. Estes passam a servir como provedores de informação, e não apenas consumidores passivos. São exemplos de aplicações *Peer-to-Peer*: *Kazaa*, *Freenet*, *Emule*, *Edonkey*, *aMule*, *Shareaza*, *LimeWire*, etc.

O engenheiro social utiliza várias técnicas para obter as informações de que necessita. Uma delas é a criar confiança nas pessoas que deseja enganar. Após adquirir esta confiança, passa a atacar e conseguir as informações. Ele prepara toda a teia de situações que podem vir a ocorrer, como questionamentos e perguntas das quais ele possa ter que responder no ato, sem gaguejar, ou demonstrar insegurança, a ponto da vítima não ter motivo de desconfiar algo estranho na pessoa.

O *hacker* pode ser considerado o primo longe do engenheiro social. Nem todo engenheiro social é um hacker, mas em alguns casos o hacker chega a ser um engenheiro social, com condutas semelhantes à captura de informações. O hacker age de forma a explorar muito mais as vulnerabilidades técnicas, enquanto o engenheiro social explora as vulnerabilidades humanas.

A internet é um excelente recurso para coleta de informações, assim como para aprimorar ataques de engenharia social. Armadilhas como sites clonados, mensagens enganosas que chegam ao correio eletrônico, denominados *fakemail* ou *Scam* (email falsos) que se passam por mensagens verdadeiras para atrair internautas. A idéia consiste em usar o nome de uma empresa ou de algum serviço conhecido na internet para convencer usuários a clicarem no link da mensagem. No entanto, esse link não aponta para o que a mensagem oferece, mas sim para um *site* falso que tem o mesmo layout de um *site* verdadeiro ou para um arquivo executável que tem a função de capturar informações da máquina da vítima.

Segundo Emerson Alecrim [19], os *scams* usam qualquer tema, porém, os mais comuns fingem ser e-mails de cartões virtuais. Nestes casos, o link para a visualização do cartão geralmente aponta para um arquivo executável e muita gente, na expectativa de ver o cartão, clica no link sem checar se este é mesmo verdadeiro.

Há também *scams* que usam como tema assuntos financeiros, como mensagens que fingem ser e-mails de bancos conhecidos solicitando ao internauta o recadastramento de informações, sob o pretexto de alguma vantagem tentadora. Caso o usuário clique no link, este o levará um *site* falso com um visual igual ou semelhante à página do banco em questão e, por isso, o internauta tende a não desconfiar que aquele endereço é falso e acaba fornecendo suas informações, inclusive senhas.

A questão é que, cada vez mais, os internautas estão tomando ciência desses golpes e os *scammers* - os criminosos que enviam as mensagens falsas - estão em constante busca de alternativas para continuar a aplicar os golpes.

Uma das técnicas encontradas é o uso do medo e do susto. Isso funciona, basicamente, da seguinte forma: uma mensagem chega à caixa de e-mails do internauta dizendo que este possui dívidas pendentes (por exemplo, em contas de telefone) ou irregularidades em algum documento (por exemplo, no CPF - **C**adastro de **P**essoa **F**ísica).

Qualquer pessoa honesta realmente fica preocupada ao receber uma notificação desse tipo e, algumas, mesmo tendo ciência dos golpes que chegam por e-mail, no momento do

susto, podem acabar acreditando na mensagem e clicam no link que a acompanha, na expectativa de obter detalhes sobre o suposto problema.

Como exemplo de mensagem falsa, a imagem a seguir é uma falsa notificação da Receita Federal. A mensagem diz que o CPF do usuário está cancelado ou pendente de regularização. Repare que o texto apresenta *links*, mas todos apontam para "*www.pandoranyx.com/VampireForum/mail/cartao0401.scr*". Veja que esse endereço não tem nenhuma ligação com o site da Receita Federal (www.receita.fazenda.gov.br). Note também que o campo "De:" da mensagem tem como emissor o e-mail "*receita@receita.fazenda.gov.br*". Essa é uma característica que pode levar o internauta a acreditar que a mensagem é mesmo verdadeira. No entanto, não é: *spammers* (pessoas que enviam SPAM) e *scammers* usam softwares capazes de enviar milhares de e-mails por minuto. Esses programas são dotados de recursos que permitem ao emissor indicar qualquer endereço como remetente. Dessa forma, uma mensagem falsa pode ter o campo "De:" preenchido com um endereço da Receita Federal, do FBI, do *InfoWester*, enfim, de qualquer site. Se o cabeçalho dessas mensagens for analisado, será possível constatar que a emissão não foi feita pelo endereço indicado anteriormente.

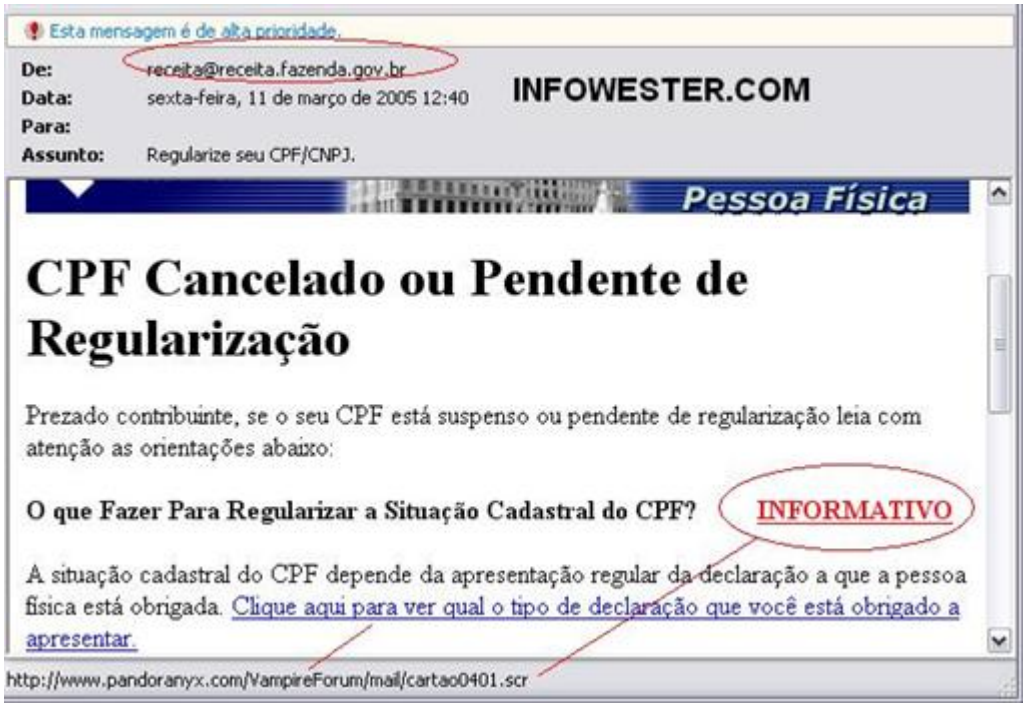


Figura 2.6 - Imagem de um e-mail falso (*scam*) [ALECRIM, 2005]

2.9.1. Engenheiro Social versus Security Officer

Segundo Mário César Peixoto [10], o *Security Officer* não deixa de ser um engenheiro social do bem, devido a ter que conhecer suas técnicas, seu modo de agir, enfim, o perfil com atitudes e suspeitas de que esteja se deparando com um ataque da engenharia social, caso este suposto engenheiro social esteja realmente aplicando suas habilidades por um propósito maléfico. O *Security Officer* utiliza técnicas e ferramentas que muitas vezes o engenheiro social mal intencionado utiliza, para detectar, demonstrar e descobrir as fragilidades existentes (ou o chamado elo mais fraco) dentro da organização e poder assim tomar medidas aplicáveis a evitar ou dificultar o que antes era um ponto de vulnerabilidade.

Contudo, infelizmente, existe não somente o lado da curiosidade, impetuosidade ou "vontade de descobrir o que não pode", mas sim o lado da maldade, do rancor e até mesmo da vingança, que o ser humano carrega consigo transpondo as barreiras do bom senso, da responsabilidade e, sobretudo, a do respeito, fazendo com que tais habilidades sejam utilizadas na "arte de enganar" pessoas. Serão abordadas algumas medidas que o *Security Officer* e sua equipe de segurança poderão implementar como medidas de controle de segurança, assim como treinamentos e sensibilização.

2.9.2. Solução Corporativa de Segurança da Informação

Segundo Marcos Sêmola, a Solução Corporativa de Segurança da Informação é o resultado da criação de uma estrutura corporativa adequadamente posicionada no organograma denominada Comitê Corporativo de Segurança da Informação, baseado em um modelo de gestão dinâmico, com autonomia e abrangência, coordenado por um executivo em ação focada intitulado *Security Officer*. O *Security Officer* tem que ser o mediador, orientador, questionador, analisador de ameaças, impactos e consequentemente responsável por um estudo de viabilidade para cada situação e etapas a serem impostas, na esfera das estratégias de análise dos riscos [1]. Este, apoiado por uma equipe própria ou terceirizada, e por representantes de departamentos ou gestores dos processos críticos, orientados por um Plano Diretor de Segurança desenvolvido sob medida e alinhado às diretrizes estratégicas do negócio, que irá organizar as atividades em busca da adoção de controles que conduzam os riscos ao patamar operacional definido como ideal.

Realmente não é tarefa fácil elaborar e executar um Plano Diretor de Segurança, mas bastante possível na medida em que se conheçam verdadeiramente os negócios da empresa tendo a liberdade de propor novos planos à Diretoria. Sem entrar especificamente em detalhes sobre cada

processo, será apenas mencionado cada um (apenas como uma visão "top-down"); sabendo-se da grande importância que existe para o *Security Officer* de aplicar tais processos, cada um com suas particularidades:

- Solução Corporativa de Segurança da Informação;
- Plano Diretor de Segurança;
- Plano de Continuidade de Negócios;
- Política de Segurança da Informação;
- Análise de Riscos e Vulnerabilidades;
- Testes de Invasão;
- Implementação de Controles de Segurança;
- Treinamento e Sensibilização em Segurança;
- Equipe para Resposta a Incidentes;
- Administração e Monitoração de Segurança.

Cada caso é um caso, em detrimento ao que será implementado como processo para cada empresa. Entende-se então que não existe uma solução padrão para ser aplicada em todas as empresas e sim planos personalizados conforme a necessidade de cada uma.

2.10. PROPOSTAS DE SEGURANÇA

Tendo que se preocupar com a segurança em diversos aspectos, sendo o tecnológico muita das vezes o foco de principal atenção a ser lembrado, fica dispersa a implementação de controles de segurança, principalmente relativa aos outros dois: físicos e humanos. Aos poucos se percebe que não mais está sendo tão comum essa cultura de "esquecer" estes outros dois fatores, como também delimitadores da emergente necessidade de investir maiores esforços quanto à aplicabilidade aos mecanismos de controle de segurança a fim de atingir o nível de risco adequado.

Quanto aos riscos inerentes aos fatores humanos**,** podem-se destacar como exemplo os seguintes controles:

- Seminários de sensibilização;
- Cursos de capacitação;
- Campanhas de divulgação da política de segurança;
- Crachás de identificação;
- Procedimentos específicos para demissão e admissão de funcionários;

- Procedimentos específicos para tratamento de recursos terceirizados;
- Termo de responsabilidade;
- Termo de confidencialidade;
- *Softwares* de auditoria de acessos;
- *Softwares* de monitoramento e filtragem de conteúdo.

Quanto aos riscos inerentes aos fatores físicos**,** para um melhor controle e proteção, podemos citar:

- Roletas de controle de acesso físico;
- Climatizadores de ambiente;
- Detectores de fumaça;
- Acionadores de água para combate a incêndio;
- Extintores de incêndio;
- Cabeamento estruturado;
- Salas-cofre;
- Dispositivos de biometria;
- Certificados Digitais de Token;
- Circuitos internos de televisão;
- Alarmes e sirenes;
- Dispositivos de proteção física de equipamentos;
- *Nobreaks*;
- Dispositivos de armazenamento de mídia magnética;
- Fragmentadoras de papel.

2.10.1. Dificultando a Vida do Engenheiro Social

A maior prova para se ter certeza de que você será a próxima vítima da engenharia social é simplesmente subestimar o praticante desta arte. Mas como ao certo saber quem é afinal o engenheiro social naquele dado momento, lugar ou situação? Não saberá, na primeira instância. Apenas desconfiará de algum suspeito à medida que você vá adquirindo conhecimento das técnicas padrões e revolucionárias da engenharia social. E assim percebendo algumas "gafes" do engenheiro social, deixará a incerteza para então capturar o alvo certo.

Mas a equipe de segurança, ou o *Security Officer* pode muito bem dificultar a vida deste audacioso elemento, que não mais será surpresa e sim presa fácil, se aplicada a já mencionada

técnica da *engenharia social reversa* (para isso deverão existir profissionais treinados e preparados para executar tal procedimento) mais alguns métodos de autenticação que podem ser divididos em três grupos, segundo o grau de segurança que oferecem.

1. O que você sabe?
2. O que você tem?
3. O que você é?

2.10.2. O que você sabe

Método baseado na utilização de senhas. Não deixa de ser uma maneira para dificultar a entrada não autorizada, mas definitivamente não é o mais eficiente e seguro. Consiste em não colocar as chamadas "senhas fortes", onde se tenha no mínimo seis dígitos com números e letras misturados e que não lembre nada do mundo real, como: nomes próprios, placas de automóvel, datas de nascimento dentre outros. Nativamente este método já revela fragilidades, pois a segurança depende de fatores internos como a estrutura de construção e manutenção da senha, bem como de fatores externos ao método como o comportamento dos agentes que podem ter desvios de conduta, levando ao comprometimento do mecanismo. Compartilhar a senha, selecionar uma senha fraca, não mantê-la em segredo ou, ainda, manuseá-la sem os critérios adequados, podem por em risco toda a eficiência do método.

Desmistificando a classificação popular de senha fraca ou forte, tome como base os critérios de classificação Acadêmica e Prática. Academicamente falando, uma senha pode ser classificada como forte se possuir mais de seis caracteres, misturar números, letras em maiúsculo, em minúsculo e caracteres especiais como colchete, asterisco etc. E pode ser classificada como fraca se possuir menos de seis caracteres, se for construída apenas por números, letras maiúsculas ou minúsculas e, principalmente, quando, apesar de possuir tamanho maior, representar alguma informação do mundo real, ou seja, nomes próprios, placa de automóveis, datas de nascimento etc.

Em contrapartida, adotando o critério prático de classificação, uma senha pode assumir o rótulo de forte ou fraca dependendo, fundamentalmente, de três fatores: do valor e importância das informações protegidas por ela, do tempo em que a senha estará cumprindo o papel de proteção, e pelo poderio, interesse e disposição que um suposto interessado despenderia para obter acesso à informação protegida.

2.10.3. O que você tem

Baseado na utilização de dispositivos físicos para facilitar de forma mais confiável as autenticações de acesso. Método aplicado conforme também as necessidades do nível de segurança desejado; além do orçamento disponível para implementar determinada tecnologia. Vem sendo adotado de forma crescente baseado na utilização de dispositivos físicos que são apresentados em processos de autenticação de acessos. Há um grande conjunto de dispositivos que se encaixam neste perfil. A escolha do melhor mecanismo está diretamente atrelada ao nível de segurança necessário para as informações e inevitavelmente ao orçamento disponível.

- Cartão com código de barras;
- Cartão magnético;
- *Smartcard*;
- *Tokens*, etc.

2.10.4. O que você é

Ainda em fase de popularização e barateamento, este método emprega dispositivos físicos que realizam métricas biométricas para identificar pessoas que exercem o direito de acesso a informações, ambientes etc. Costumeiramente, são equipamentos dispendiosos devido à tecnologia de ponta empregada, pois se baseiam na leitura de informações do corpo humano, que são únicas em cada indivíduo. O nível de segurança oferecido por cada dispositivo depende diretamente da métrica usada e do número de pontos de comparação disponíveis por cada parte do corpo analisado.

Geralmente um dos métodos mais caros, mas também um dos mais eficientes, consiste em empregar dispositivos físicos que realizam métricas biométricas para identificar pessoas que exercem o direito de acesso a informações, lugares etc.

- Geometria das mãos;
- Geometria da face;
- Identificação digital;
- Reconhecimento da voz;
- Leitura de íris, etc.

A idéia sem dúvida é dificultar ao máximo que puder a concretização dos planos que o engenheiro social tem em mente e deseja pôr em prática. Pois como o maior entendido do

assunto, Kevin Mitnick, havia dito: *"A verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social"* [17].

O importante é que deve haver a conscientização por parte de todos os empregados, para assim ao menos amenizar as ameaças da engenharia social. E esta conscientização deverá estar sendo combinada às políticas de segurança, juntamente com os hábitos das condutas corretas segmentadas às regras definidas, completando com treinamentos.

Funcionários treinados e conscientes fazem com que aumente de forma considerável o conhecimento baseado nas políticas de segurança adotadas pela organização e as técnicas utilizadas pelo engenheiro social. Quanto maior este conhecimento, maior será a resistência de se cair nas armadilhas do engenheiro social. *"Algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização"*.

Diante de tantas opções de autenticação e da oferta de diferentes níveis de segurança proporcionados por cada método, é fator crítico de sucesso para o gestor da segurança analisar em detalhes o perímetro-alvo da autenticação, as reais necessidades de proteção impostas pela criticidade das informações e os impactos relacionados ao desempenho e montante de investimento demandado. Mesmo assim, podem surgir situações em que um único método não atenda aos requisitos mínimos de segurança, tornando necessário combinar um ou mais métodos. Estas soluções híbridas têm sido uma constante em segmentos específicos, como o financeiro, onde o cliente, além de possuir um cartão magnético, tem de inserir uma senha fixa e, ainda, informações pessoais de comprovação de identidade.

2.10.5. Plano de treinamento

Os recursos humanos são considerados o elo mais frágil da corrente, pois são responsáveis por uma ou mais fases de processo de segurança da informação. Esta situação é ratificada pelo fato de o *peopleware* não ter um comportamento binário e previsível em que se possa eliminar todas as vulnerabilidades presentes. O ser humano é uma máquina complexa, dotada de iniciativa, criatividade e que sofre interferência de fatores externos, provocando comportamentos nunca antes experimentados. O fator surpresa é um dos pontos nevrálgicos dos processos de segurança que dependem das pessoas. Se especificarmos normas de criação, manuseio, armazenamento, transporte e descarte de senhas, implementamos recursos tecnológicos de auditoria e autenticação de acesso para tornar um ambiente mais seguro, podemos ter a eficiência dessas iniciativas postas em dúvida à medida que um recurso

humano descumpra as instruções da política de segurança e compartilhe sua senha supostamente pessoal e intransferível.

Esses riscos precisam ser tratados de forma gradativa, objetivando formar uma cultura de segurança que se integre às atividades dos funcionários e passe a ser vista como um instrumento de autoproteção. As ações devem ter a estratégia de compartilhar a responsabilidade com cada indivíduo, transformando-o em co-autor do nível de segurança alcançado. Somente desta forma as empresas terão, em seus funcionários, aliados na batalha de redução e administração dos riscos.

Muitas são as formas de iniciar a construção da cultura de segurança. Algumas delas se aplicam a públicos com perfis diferentes; outras se aplicam a todos os perfis, mas em momentos distintos.

Fazer um raio-x das problemáticas e deficiências existentes dentro da organização, diagnosticando setores frágeis quanto à segurança, percebendo que a estrutura em si está comprometida a qualquer momento de sofrer um ataque da engenharia social sem ter os "anticorpos" necessários a se defender, é algo a que o *Security Officer* deve ficar atento.

Para tanto, a estrutura do treinamento a ser aplicado a *todos* os funcionários deverá levar consigo já dois princípios básicos que poderiam evitar alguns ataques, conforme observou Mitnick:

1. Verificar a identidade da pessoa que faz a solicitação; ou seja, essa pessoa é realmente quem diz ser?
2. Verificar se a pessoa está autorizada; ou seja, a pessoa tem a necessidade de saber ou tem autorização para fazer a solicitação?

Conforme observou Mitnick [17], um bom e prático programa de treinamento e conscientização visando a segurança das informações contidas também os aspectos do comportamento humano pode incluir:

- Uma descrição do modo como os atacantes usam habilidades da engenharia social para enganar as pessoas;
- Os métodos usados pelos engenheiros sociais para atingir seus objetivos;
- Como reconhecer um provável ataque da engenharia social;
- O procedimento para o tratamento de uma solicitação suspeita;
- A quem relatar as tentativas da engenharia social ou os ataques bem sucedidos;

- A importância de questionar todos os que fazem uma solicitação suspeita, independentemente da posição ou importância que a pessoa alega ter;
- O fato de que os funcionários não devem confiar implicitamente nas outras pessoas sem uma verificação adequada, embora o seu impulso seja dar aos outros o benefício da dúvida;
- A importância de verificar a identidade e a autoridade de qualquer pessoa que faça uma solicitação de informações ou ação;
- Procedimentos para proteger as informações confidenciais, entre eles a familiaridade com todo o sistema de classificação de dados;
- A localização das políticas e dos procedimentos de segurança da empresa e a sua importância para a proteção das informações e dos sistemas de informações corporativas;
- Um resumo das principais políticas de segurança e uma explicação do seu significado. Por exemplo, cada empregado deve ser instruído sobre como criar uma senha difícil de adivinhar;
- A obrigação de cada empregado de atender às políticas e as conseqüências do seu não-atendimento.
- A motivação para que o funcionário aplique de forma mais eficaz tais medidas de segurança das informações é promover, por exemplo, certificados pela conclusão e acompanhamento dos programas de treinamento oferecidos pela empresa; brindes ou prêmios por estar colaborando significativamente para a diminuição dos ataques sofridos, dentre outras maneiras.
- Seria também muito importante fazer com que o funcionário assinasse algum termo de comprometimento quanto ao seguimento das políticas e princípios de segurança que foram ministrados pelo programa. Geralmente quando as pessoas assinam algo, as chances de se esforçar para cumprir os procedimentos aumentam.

2.10.6. Exemplos para Reforçar a Conscientização

Apesar de se ter em mente que os planos para o desenvolvimento de um programa de conscientização partam quase que exclusivamente do departamento de Tl, por estar envolvendo tecnologias e estruturas físicas, não se pode esquecer que envolve também principalmente o mais importante de todos: o ser humano. Então nada mais justo e coerente que desenvolver o plano de

conscientização da segurança das informações juntamente com o departamento de Recursos Humanos.

O programa de conscientização deverá ser criativo, dinâmico e convincente. Demonstrar que aquilo que está sendo posto em prática é realmente necessário e é sobretudo importante.

Portanto, assim como na propaganda tradicional, o humor e a inteligência ajudam. Fugir da mesmice de divulgações que nunca mudam, ou seja, que já se tornam bastante familiares, fazendo assim com que comecem a serem ignoradas, colabora para que fiquem mais "enraizadas" as mensagens na mente de cada um.

Seminários

O trabalho deve começar com seminários abertos voltados a compartilhar a percepção dos riscos associados às atividades da empresa, os impactos potenciais no negócio e, principalmente, o comprometimento dos processos críticos se alguma ameaça se concretizar. Desta forma, cada funcionário passa a se enxergar como uma engrenagem da máquina e co-responsável por seu bom funcionamento, podendo gerar impactos diretos ao seu processo e indiretos a processos adjacentes.

Campanha de Divulgação

É importante que a empresa disponha de uma política de segurança atualizada e alinhada às necessidades e estratégias do negócio, mas é fundamental que ela seja reconhecida pelos funcionários como o manual de segurança da empresa. Suas diretrizes devem ser conhecidas por todos, e suas normas, procedimentos e instruções específicas devem ser apresentados a cada grupo com perfil de atividade semelhante. Desta forma, cada membro percebe suas responsabilidades dentro de um modelo de segurança único, motivando-o a colaborar. Mas não é suficiente. Lembre-se de que os resultados efetivos de comprometimento ocorrem lentamente e, muitas vezes, requerem ações complementares.

Por conta disso, a campanha deverá lançar mão de diversos artifícios para comunicar os padrões, critérios e instruções operacionais, como cartazes, jogos, peças promocionais, protetores de tela, e-mails

informativos, e-mails de alerta, comunicados internos, páginas especializadas na Intranet etc.

Carta do Presidente

Como instrumento de oficialização dos interesses da empresa em adequar o nível de segurança de suas informações a partir do envolvimento de todos os níveis hierárquicos é conveniente que o presidente, CEO ou CIO externe esta vontade oficialmente. A Carta do Presidente tem esse papel e é disponibilizada, quando não, encaminhada a cada funcionário, dando um caráter formal ao movimento. Por vezes, este documento aparentemente simples, é responsável por muitos apoios espontâneos e o natural fortalecimento do plano estratégico de segurança da informação.

Termo de Responsabilidade e Confidencialidade

Considerado mais um importante instrumento de sensibilização e formação de cultura, o Termo de Responsabilidade e Confidencialidade tem o propósito de formalizar o compromisso e o entendimento do funcionário diante de suas novas responsabilidades relacionadas à proteção das informações que manipula. Além disso, este termo se encarrega de divulgar as punições cabíveis por desvios de conduta e, ainda, esclarecer que a empresa é o legítimo proprietário dos ativos, incluindo as informações, que fluem pelos processos de negócio e ora são temporariamente custodiadas pelas pessoas.

Cursos de Capacitação e Certificação

Dentro do quadro de funcionários, existem perfis profissionais que necessitam de maior domínio dos conceitos, métodos e técnicas de segurança, podendo inclusive, variar sua área de interesse e profundidade. Os administradores de rede, por exemplo, precisam estar preparados para reagir às tentativas de ataque e invasão, ou para contingenciar situações de risco. O *Security Officer*, por sua vez, deve ter condições de definir, medir e avaliar os índices e indicadores de segurança para subsidiar seus planos de gestão e seu planejamento de trabalho, a fim de garantir a total integração das ações e, principalmente, alcançar os objetivos. Para todos esses casos, não bastam os seminários, campanhas de conscientização ou a carta do presidente. Eles precisam de Capacitação formal através de cursos especializados, que propõem uma certificação como instrumento de reconhecimento da competência. Pela heterogeneidade de perfis, surgem demandas de cursos verticalmente técnicos, voltados a capacitar recursos em uma determinada tecnologia de segurança, bem como demandas para orientação e preparação de *Security Officers.* Entretanto, é relevante destacar a necessidade de processos contínuos de sensibilização e Capacitação das pessoas,

sob pena de ter a equipe estagnada e, brevemente, despreparada para a administração das novas situações de risco.

Alguns exemplos para reforçar a concretização de um plano constante de conscientização podem incluir:

- O fornecimento de trabalhos, pesquisas, artigos para leitura voltados à engenharia social, para todos os funcionários;
- A inclusão de itens informativos nas circulares da empresa: por exemplo, artigos, lembretes (de preferência itens curtos que chamem a atenção) ou quadrinhos;
- A colocação de uma foto do funcionário da Segurança do mês;
- Pôsteres afixados nas áreas dos empregados;
- Notas publicadas no quadro de avisos;
- O fornecimento de lembretes impressos nos contracheques de pagamento;
- O envio de lembretes por correio eletrônico;
- O uso de proteções de tela relacionadas com segurança;
- A transmissão de anúncios sobre a segurança por meio dos sistemas de *voice mail*;
- A impressão de etiquetas para o telefone com mensagens tais como: "A pessoa que está ligando é quem ela diz ser"?;
- A configuração de mensagens de lembrete que aparecem quando o computador é ligado, tais como: "Criptografe as informações confidenciais antes de enviá-las";
- A inclusão da conscientização para a segurança como o item-padrão nos relatórios de desempenho dos empregados e nas análises anuais;
- A publicação na intranet de lembretes de conscientização para a segurança, talvez usando quadrinhos ou humor, ou alguma outra maneira que incentive as pessoas a lerem;
- O uso de um quadro eletrônico de mensagens na lanchonete, com um lembrete de segurança que seja trocado freqüentemente;
- A distribuição de folhetos ou brochuras;
- E pense naqueles biscoitos da sorte que são distribuídos de graça na lanchonete, contendo cada um deles um lembrete sobre a segurança em vez de uma previsão.

Toda precaução e divulgação quanto à segurança são válidos. Assim como as ameaças são constantes, os lembretes também devem ser constantes.

2.10.7. Atuação do Security Officer

Assim como o chamado *ombudsman, o Security Officer* é a pessoa responsável por criticar, argumentar e questionar fatos e fatores, casos e ocorrências, sendo às vezes conhecido como o indivíduo "chato" da organização.

Algo interessante seria a empresa contratar uma pessoa desconhecida por todos que nela trabalham a fim de ser basicamente um "espião" colaborador às exigências impostas e determinadas pelo *Security Officer* e sua equipe de segurança. Esse trabalho seria feito periodicamente de tempos em tempos (conforme a necessidade emergente, ou até mesmo pela rotina padrão que fora determinada pelo *Security Officer).* Deve constar no contrato que este profissional espião estabeleça total acordo de confidencialidade a todas as informações repassadas, assim como principalmente as descobertas de vulnerabilidades detectadas por ele, pelo fato agora deste ser também um funcionário da empresa (mesmo sem estar trabalhando com a periodicidade de costume, dos demais empregados).

O papel do *Security Officer* não ficaria ofuscado de maneira alguma com a presença deste espião. Seria apenas mais uma poderosa ferramenta para ajudar na diminuição de pontos vulneráveis que possam mais tarde se tornar ameaças crônicas resultando em impactos às vezes irreparáveis.

O surgimento deste novo tipo de profissional poderá vir a crescer daqui a alguns anos, mediante a verdadeira tônica da insegurança crescente que se alastra cada vez mais, pondo em cheque a estabilidade de qualquer organização.

Seguindo três critérios de verificação relevantes quanto à ajuda na identificação de determinada pessoa que solicita alguma informação, faz com que as possibilidades desta pessoa conseguir enganar ou convencer sejam menores. Os critérios seriam os seguintes:

- Verificação da identidade;
- Verificação do *status* do empregado;
- Verificação da necessidade de saber.

A *verificação da identidade* poderia estabelecer os seguintes recursos como fatores dificultantes ao praticante da engenharia social:

- Identificador de chamadas, realizando posteriormente também uma ligação de retorno;
- Realizar um modo de Autorização, onde se verifica realmente se determinado solicitante tem o consentimento de alguém de confiança da empresa;

- Utilizar do chamado "segredo compartilhado", como por exemplo um código diário ou uma senha (isto é, uma *IGD Interna);*
- Utilizar o e-mail seguro, que é uma forma de mensagem assinada digitalmente;
- Fazer o reconhecimento pessoal de voz, como por exemplo, já ter falado pessoalmente com essa pessoa, conhecendo a verdadeira voz do outro lado da linha;
- Outro recurso é a de se apresentar pessoalmente com identificação, ou seja, além de estar lá de corpo presente, tem também que mostrar o crachá para se identificar (de preferência com foto).

Na *verificação do status do empregado,* algumas outras medidas à parte devem ser levadas em conta. Sempre atente-se àquele ex-funcionário. O empregado demitido é tão perigoso quanto o Engenheiro Social, pois, infelizmente, pode haver o sentimento de vingança e descontentamento por parte deste funcionário demitido, levando informações importantes da empresa.

Vejamos alguns métodos para verificar a autenticidade deste solicitante de informações, sabendo se é ou não ainda um integrante da empresa:

- Fazer uma verificação na lista de empregados que estão em atividade, ou verificar naquele mês a relação de empregados demitidos ou admitidos;
- Realizar a verificação com o gerente do solicitante;
- Verificação do departamento ou grupo de trabalho do solicitante.

Por fim, a *verificação da necessidade de saber* considera algo simples a ser questionado: "Por que você quer saber sobre isso?".

Algumas formas que ajudam a diminuir esse gargalo e filtrar a passagem somente daqueles que na verdade são reconhecidos e autorizados têm como alguns métodos

- Consultar a lista de cargos, grupos de trabalho e/ou responsabilidades;
- Obter autorização de um gerente;
- Obter a autorização do proprietário ou criador das informações.

Em síntese, o *Security Officer* deverá saber identificar alguns sinais de ataque do Engenheiro Social**,** tais como, por exemplo:

- Recusa em dar um número de retomo;
- Solicitação fora do comum;
- Alegação de autoridade;
- Ênfase na urgência;
- Ameaças de conseqüências negativas em caso de não atendimento;

- Mostrar desconforto quando questionado;
- Nome falso;
- Cumprimentos ou lisonja;
- Flerte.

2.10.8. Penalidades e Processos Disciplinares

Nenhuma Política de Segurança pode ser estabelecida sem estas considerações. Os executivos devem demonstrar que punições severas serão aplicadas aos colaboradores da organização (estagiários, prestadores de serviço, funcionários etc.) que desrespeitarem ou violarem as políticas internas. Essa severidade será determinada em função do grau de problemas e ou prejuízos atribuídos à organização. Pode-se simplesmente mudar as atividades realizadas por um determinado profissional e, em casos graves, realizar sua demissão e aplicar as sanções legais.

O principal objetivo de estabelecer punições pelo não-cumprimento da política é incentivar os usuários a aderirem a ela e também dar respaldo jurídico à organização.

Qualquer violação deve ser imediatamente levada ao conhecimento da Alta Administração. A área de Segurança da Informação, bem como os responsáveis pelas áreas de negócio, deverão assegurar que o problema da violação foi resolvido e executar as ações necessárias para evitar reincidências.

A própria Política de Segurança deve prever os procedimentos a serem adotados para cada caso de violação, de acordo com sua severidade, amplitude e tipo de infrator que a executa. A punição pode ser desde uma simples advertência verbal ou escrita até uma ação judicial.

Atualmente, existem leis que prevêem penas para os casos de:

- Violação de integridade e quebra de sigilo de sistemas informatizados ou bancos de dados;
- Inserção de dados falsos em sistemas de informação;
- Modificação ou alteração não autorizada de sistemas;
- Divulgação de informações sigilosas ou reservadas;
- Fornecimento ou empréstimo de senha que possibilite o acesso de pessoas não autorizadas a sistemas de informações.

Fica ainda mais evidente a importância da conscientização dos funcionários quanto à Política de Segurança da Informação. Uma vez que a Política seja de conhecimento de todos, não

será admissível que as pessoas aleguem o desconhecimento das regras nela estabelecidas a fim de se livrar da culpa sobre as violações cometidas.

Quando detectada uma violação, é preciso averiguar suas causas, conseqüências e circunstâncias nas quais ocorreu. Pode ter sido derivada de um simples acidente, erro ou mesmo desconhecimento da política, como também de negligência, ação deliberada e fraudulenta. Essa averiguação possibilita que as vulnerabilidades até então desconhecidas pelo pessoal da gerência de segurança passem a ser consideradas, exigindo, se for o caso, alterações nas políticas.

2.10.9. Conclusão

A questão da privacidade estar cada vez menor, ao ponto de daqui a alguns anos quase não mais existir, é fato. As informações, sejam elas pessoais ou empresariais, estão cada vez mais fáceis de serem encontradas e utilizadas.

O patamar em que se encontram tais informações sendo expostas da forma que são, tão facilmente divulgadas e compartilhadas, não está definitivamente no mesmo patamar da noção e conscientização das pessoas físicas e jurídicas com relação a esta "imprivacidade" que delas detêm.

Programar diversos mecanismos de identificação, autorização, armazenamento de dados, sistemas de auditoria, inspeção e Checagem ajudam. E devem ser levados em conta, para que haja maior segurança quanto à exposição involuntária ou não de informações pessoais e técnicas, enfim, confidenciais.

A árdua tarefa de ser este "super-homem" ou de se ter a "superequipe" é algo realmente difícil. Adquirir um nível de profissionais com alta capacidade de bom relacionamento interpessoal e ao mesmo tempo bons conhecimentos técnicos, está complicado. O investimento não é pouco, e muito menos com retorno em curto prazo. Mas compensa na medida em que se valorizem cada vez mais todos os ativos da empresa.

O desafio é grande e a caminhada para o "sossego" de obter definitiva segurança das informações está muito longe. Principalmente devido à falta de privacidade, cada vez maior. Mas quanto à segurança corporativa das informações deve, sem sombra de dúvidas, ser encarada como "preciosidade" cada vez mais valorizada por cada funcionário da organização.

Contudo, ter em mente que para se obterem profissionais aptos a trabalhar com esta segurança que as informações merecem ter, assim como fazer com que as pessoas que trabalhem com algum meio tecnológico principalmente sejam envolvidas a interagirem participativamente

às responsabilidades quanto às condutas ao tratamento das informações que manipulam, é um investimento a ser aplicado e não simplesmente mais uma despesa a ser adicionada ao orçamento.

3. SEGURANÇA DA INFORMAÇÃO NO SENADO FEDERAL

3.1. VISÃO GERAL

Segundo a Norma NBR ISO/IEC 17799 [12], é essencial que uma organização identifique os seus requisitos de segurança. Para tanto, existem três fontes principais:

1. Avaliação de riscos dos ativos da organização;
2. legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, parceiros, contratados e prestadores de serviço têm que atender;
3. conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Foge do escopo deste trabalho a realização de levantamento dos requisitos de segurança no Senado Federal, já que é um assunto abrangente e o autor não dispõe de recursos técnicos, conhecimento especializado e tempo para tal empreendimento.

Quanto ao item 2, foi realizada uma pesquisa de normas internas e legislação federal em vigor sobre o assunto. Essas normas e leis estão explicitadas no capítulo 10. Ressalto que não foi encontrado nos bancos de dados de normas e legislação (Nadm: Normas Administrativas) uma Política de Segurança da Informação no Senado Federal. Esse fato foi corroborado por meio de entrevistas a chefes de serviço, diretores e servidores de diversos órgãos da Casa, em que alguns desconhecem norma regulamentadora sobre o assunto e outros afirmam que não há uma Política de Segurança para a instituição (foram entrevistados servidores da Secretaria Especial de Informática – Prodasen, Secretaria Especial de Editorações e Publicações – Seep, Secretaria Especial do Interlegis, Secretaria de Segurança, Secretaria de Documentação e Informação do Senado Federal).

A ausência de uma norma que trate sobre Gestão de Segurança no Senado Federal acarreta vulnerabilidades, incongruências e outros problemas em diversos setores. Dentre os problemas mais visíveis, podemos citar:

1. não unificação de medidas de segurança por parte dos órgãos do Senado Federal. Cada órgão que compõe a estrutura organizacional do Senado estabelece suas medidas de segurança, quando elas existem. Medidas de controle são adotadas de forma diferente para o mesmo tipo de funcionários. Por exemplo, na Secretaria Especial de Informática – Seep, que cuida da impressão gráfica do Senado, os estagiários e terceirizados não têm acesso a Internet, o que não ocorre para diversos outros setores da Casa.

2. não há classificação da informação, ou seja, não há norma regulamentadora que indique a importância, a prioridade e o nível de proteção dos documentos impressos e eletrônicos.

3. não há uma definição explícita das proibições que envolvam segurança da informação e punições para os funcionários em geral. Exemplo recente que ocorreu no Senado foi o bloqueio do MSN Messenger para todos os funcionários da Casa, a menos que houvesse justificativa provando a necessidade de tal ferramenta para o trabalho. No entanto, como não há uma norma regulamentadora, apenas uma 'determinação' por parte do Prodasen, este é obrigado a cumprir ordem de desbloqueio do MSN Messenger quando uma autoridade, seja por ordem impositiva ou alegação de que precisa daquela ferramenta de comunicação, determina a sua reativação. Outra vezes, funcionários conseguem burlar a determinação, seja utilizando senha de outros que têm permissão de utilizar o Messenger ou mesmo utilizando artifícios ou brechas na rede.

4. não há requisitos de segurança nos contratos de terceirização. Dessa forma, não há como cobrar das firmas prestadoras de serviço quando terceirizados praticam ações que burlam o aspecto de segurança no Senado, pois estes podem alegar o desconhecimento das suas responsabilidades de segurança. Embora os contratos de terceirização podem levantar algumas questões complexas de segurança, os controles incluídos na Política de Segurança da Informação poderiam servir como ponto de partida para contratos que envolvam a estrutura e o conteúdo do plano de gestão da segurança.

5. não há um processo formal de registro e do cancelamento de usuário para obtenção de acesso à rede, e-mail, sistemas de informação e serviços, bem com a devolução de crachá quando funcionários comissionados, terceirizados ou estagiários têm seu contrato rescindido. O controle dos terceirizados do zelo e cuidado por parte dos responsáveis que cuidam dos contratos terceirizados, denominados gestores de contrato. Os setores de Recursos Humanos do Senado, Prodasen e Seep, nem sempre comunicam ao órgão de TI a exoneração de servidores comissionados para fins de cancelamento do login e senha. A falta de norma regulamentadora cria uma brecha nesse sentido e essa vulnerabilidade pode ser explorada por ex-funcionários mal intencionados.

6. as senhas de acesso à rede não estão atreladas à lotação do servidor nem à função que ocupa no Senado. Dessa forma, quando há mudança de lotação de servidor ou alteração da sua função, os privilégios de utilização dos serviços de rede e de sistemas de informação multiusuário não é alterado de forma automática. Ocorre que, por falta de um procedimento

formal, fica a cargo da chefia do servidor a comunicação da alteração ao órgão gerente de contas do Prodasen que este em geral providencia a alteração. O problema é que, às vezes por desconhecimento ou por negligência, não ocorre a comunicação e muitas vezes, o servidor continua com os privilégios de acesso anteriores.

7. O controle de entrada física às instalações no Senado é de competência da Secretaria de Segurança. Apesar disso, um visitante pode acessar as dependências do Senado por meio da Câmara dos Deputados e vice-versa, pois não há uma barreira física separando os dois prédios. Um controle mais eficaz poderia ser levado adiante se houvesse um planejamento e ação conjunta com a segurança da Câmara dos Deputados.

Esses foram os itens percebidos numa visão geral, sem adentrar em aspectos detalhados e outros fatos sem comprovação. Contudo, a falta de uma Política de Segurança da Informação, Implementação e Auditoria constituem causa para o surgimento de inúmeras vulnerabilidades e ameaças à informação e de quem lida com ela no dia a dia.

3.2. PESQUISA SOBRE SEGURANÇA DA INFORMAÇÃO

No período de 1º de maio a 27 de julho de 2006, foi realizada uma pesquisa sobre Segurança da Informação no Senado Federal, com 28 perguntas com respostas objetivas, com o intuito de verificar qual o nível de consciência acerca desse tema na Casa. Foram distribuídos 450 formulários para servidores efetivos (47%) e comissionados (21%), estagiários (9%) e terceirizados (23%) e exercem diferentes funções e cargos nos órgãos do Senado Federal. Todos os participantes trabalham na sede do Senado Federal, em Brasília.

O objetivo da pesquisa é o de permitir a percepção quanto ao grau de conformidade que o Senado Federal tem em relação aos controles sugeridos pelo código de conduta de gestão de segurança da informação definidos pela norma NBR ISO/IEC 17799 [12]. O resultado dessa pesquisa poderá servir como parâmetro de evolução nos níveis de segurança, após a implementação de ações por parte da administração que visem alcançar o estágio de conformidade com a referida norma.

Do total dos participantes, 34% trabalham em gabinete de senador, 55% na área administrativa (Recursos Humanos, Contabilidade, Patrimônio, etc), 2% na Secretaria Especial de Informática – Prodasen, órgão responsável pela área de Tecnologia da Informação, 2% trabalham no órgão gráfico (Secretaria Especial de Editoração e Publicação), 1% no Interlegis (programa desenvolvido pelo Senado Federal, em parceria com o Banco Interamericano de Desenvolvimento (BID), de modernização e integração do

Poder Legislativo nos seus níveis federal, estadual e municipal) e 6% em outros locais, tais como comissões parlamentares e órgãos encarregados do processo legislativo.

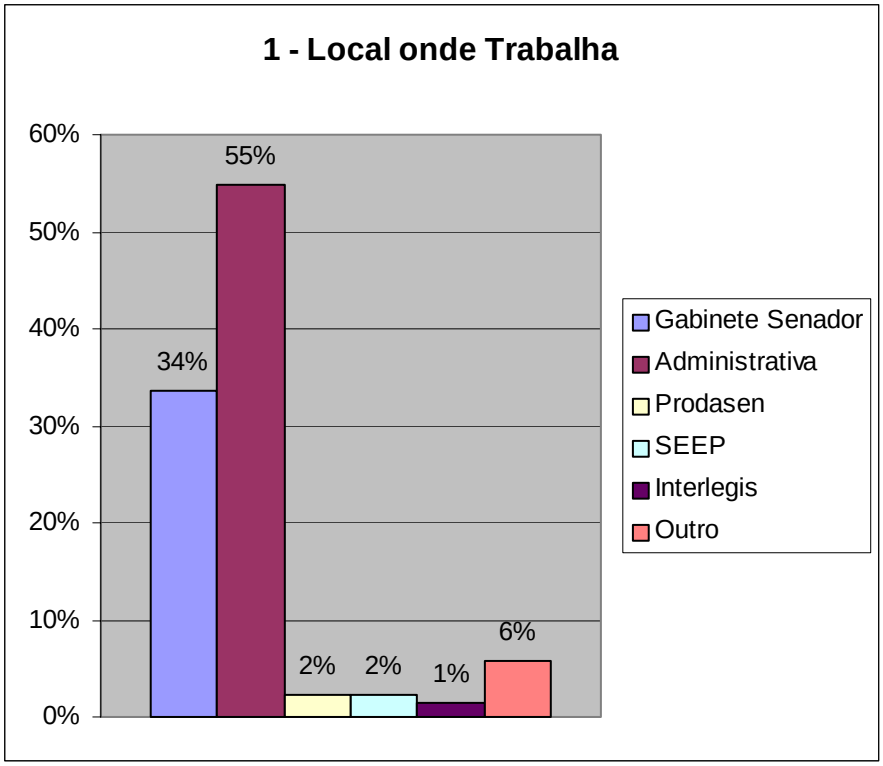


Figura 3.1 – Local onde trabalha

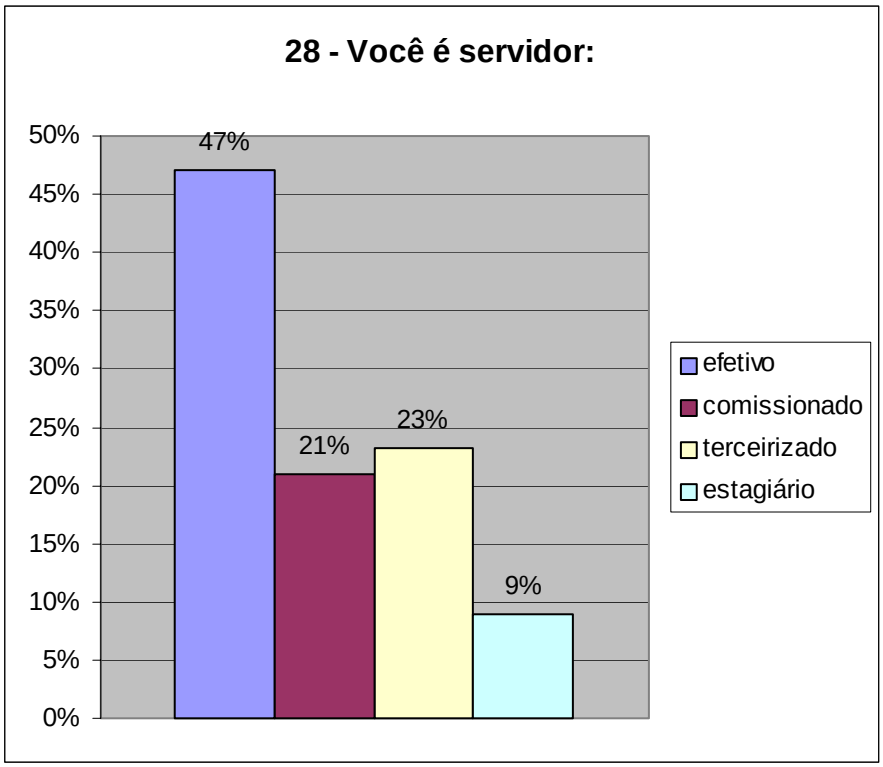


Figura 3.2 – Classificação do funcionário

Resultados

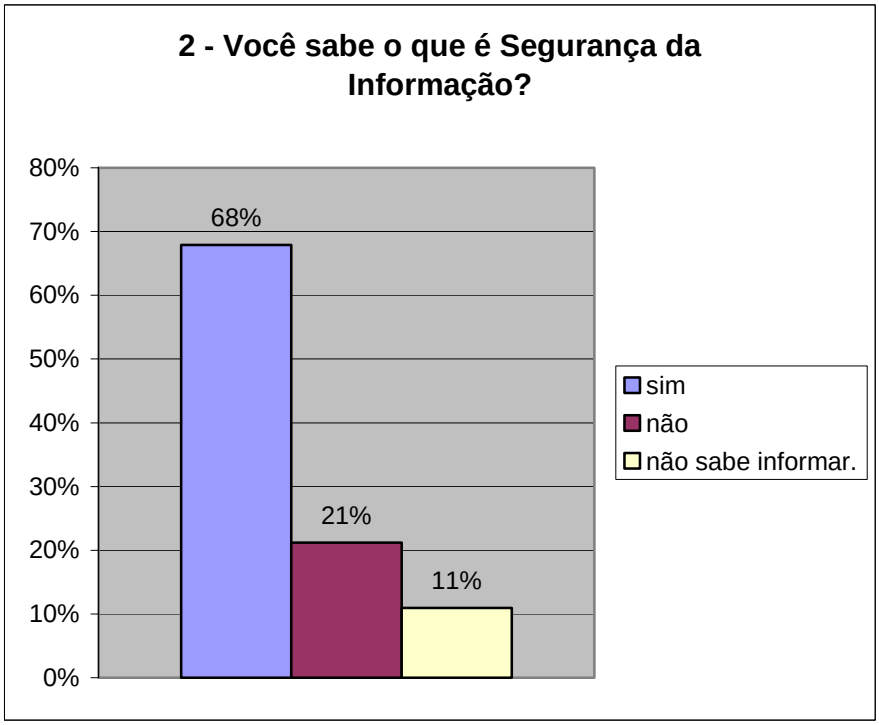


Figura 3.3 – O que é Segurança da Informação?

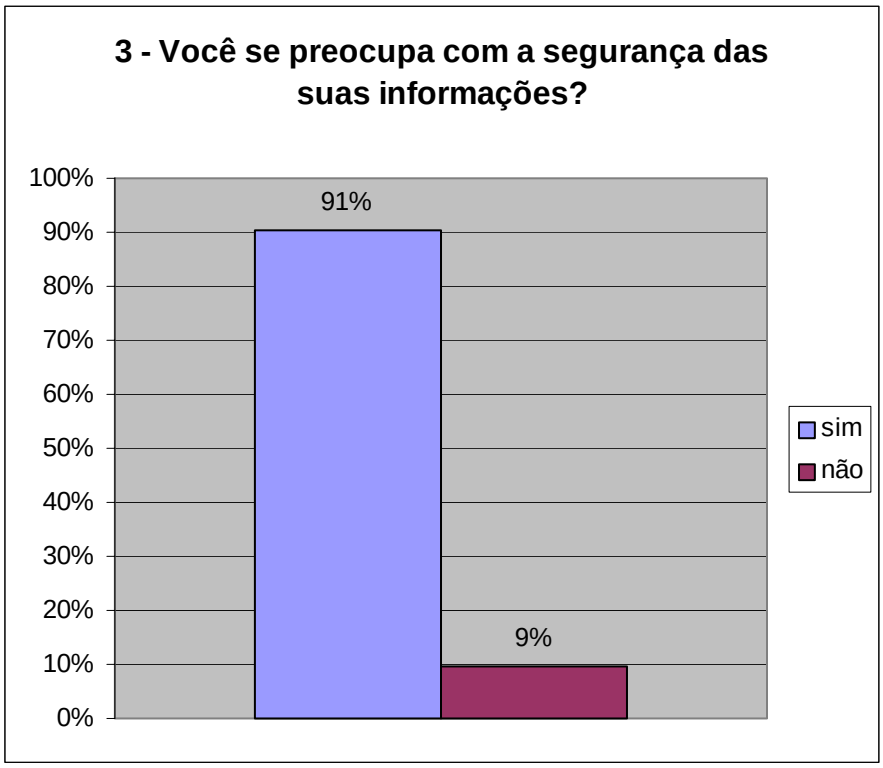


Figura 3.4 – Preocupação com a segurança da informação

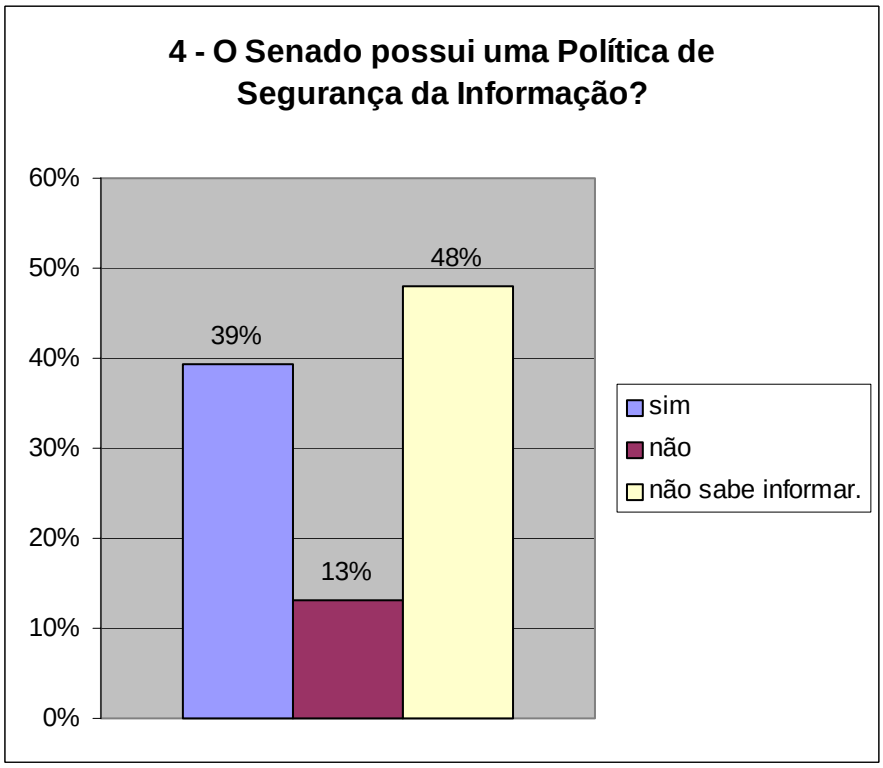


Figura 3.5 – Política de Segurança da Informação no Senado

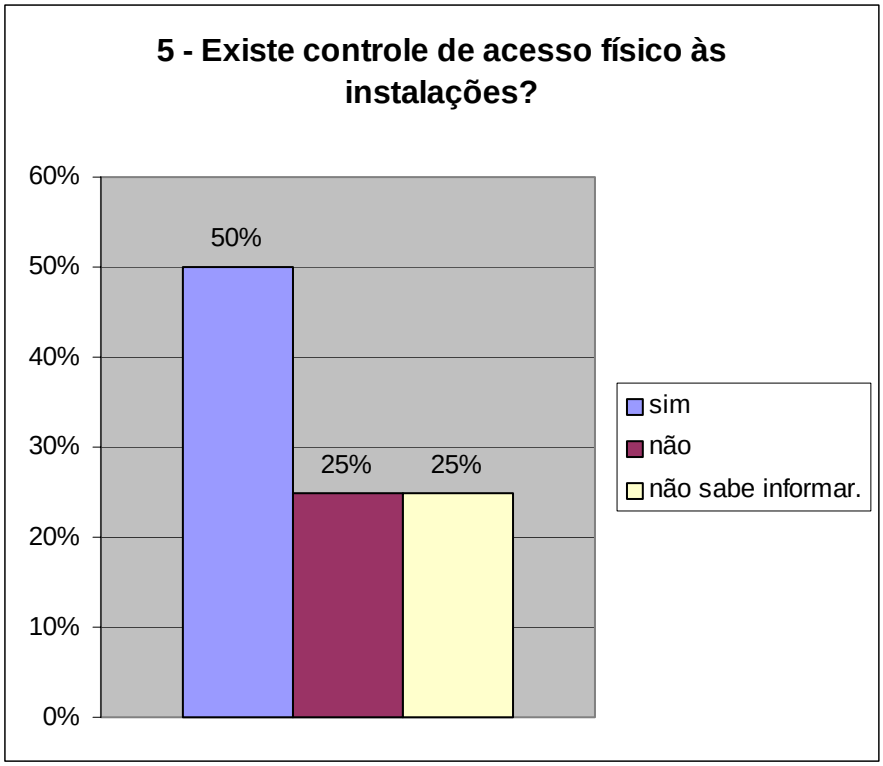


Figura 3.6 – Controle de acesso físico às instalações

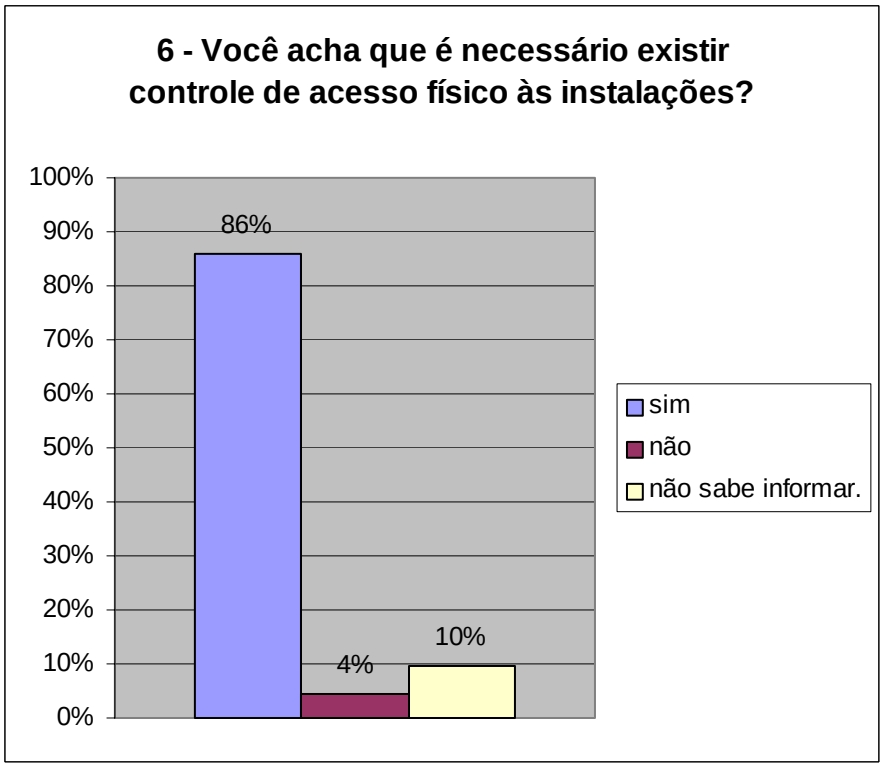


Figura 3.7 – Controle de acesso físico às instalações

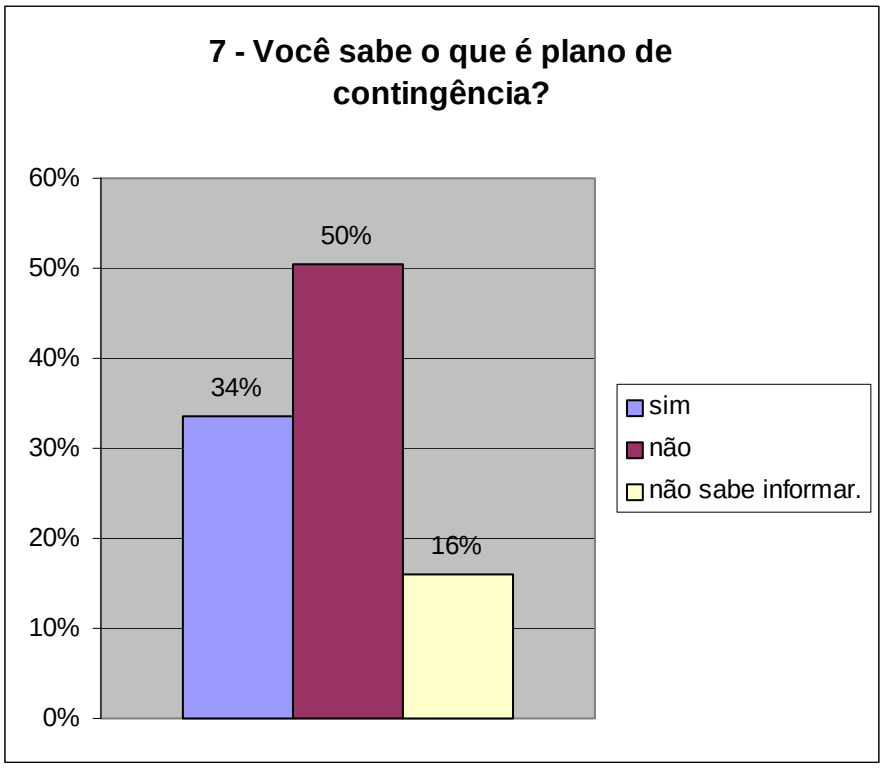


Figura 3.8 – Plano de contingência

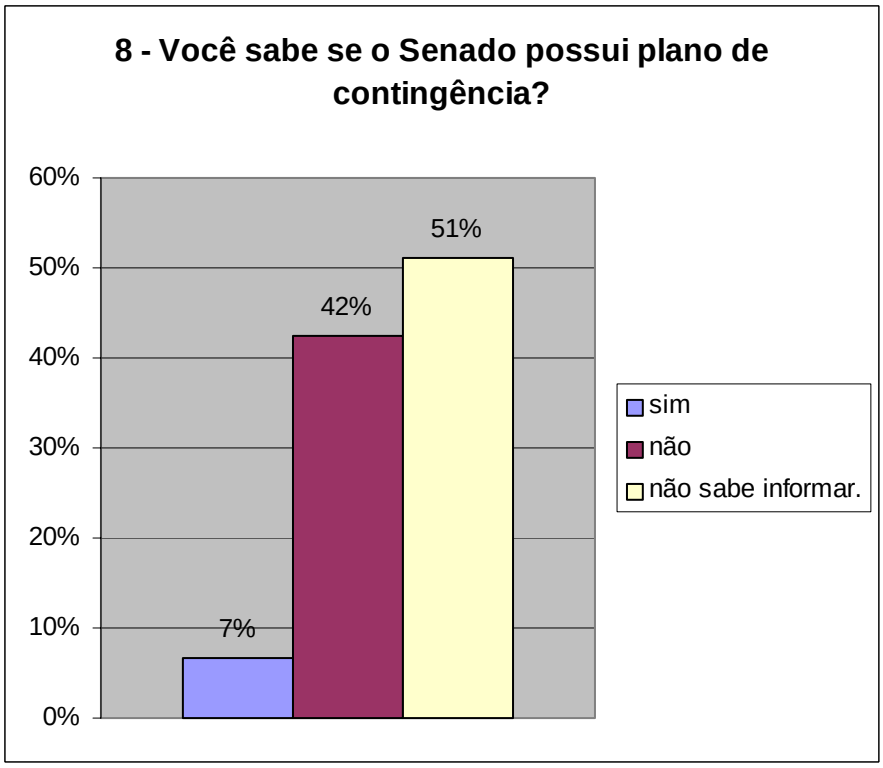


Figura 3.9 – Plano de contingência

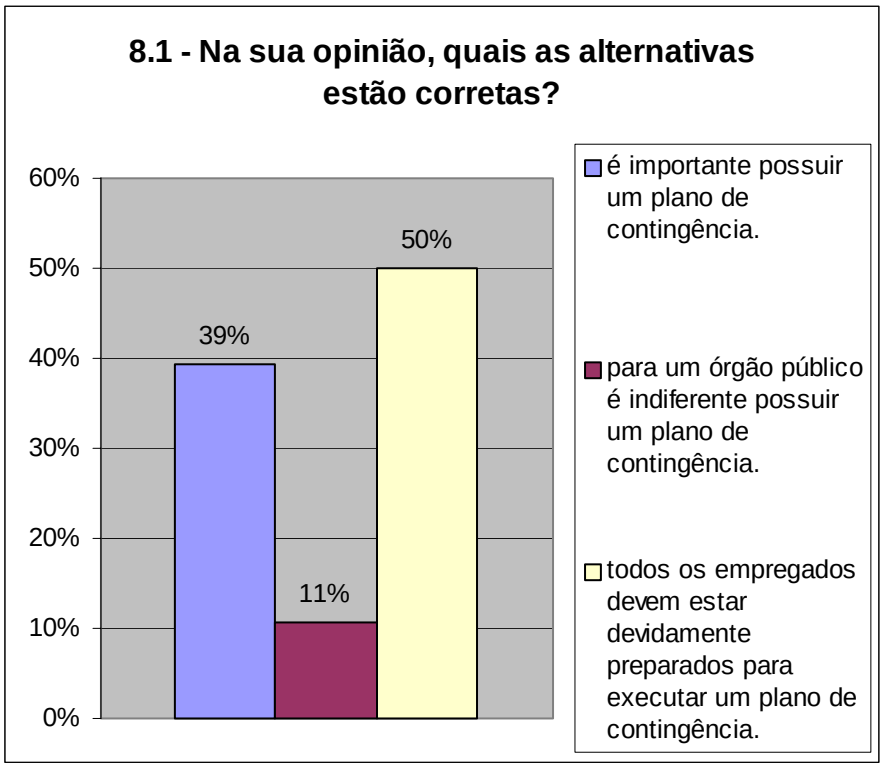


Figura 3.10 – Plano de contingência

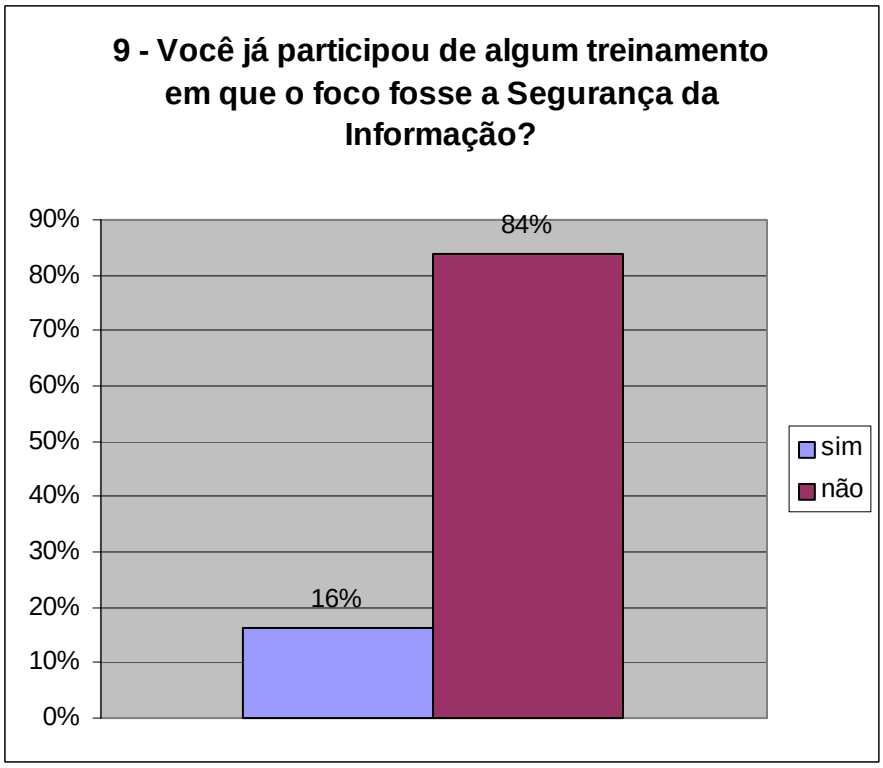


Figura 3.11 – Treinamento em Segurança da Informação

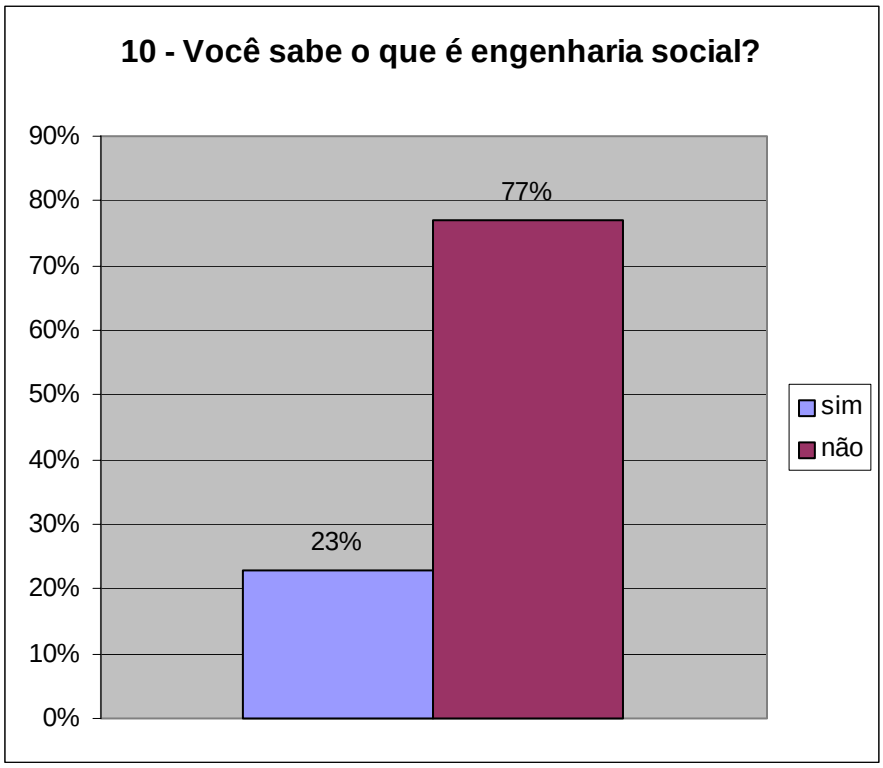


Figura 3.12 – Engenharia Social

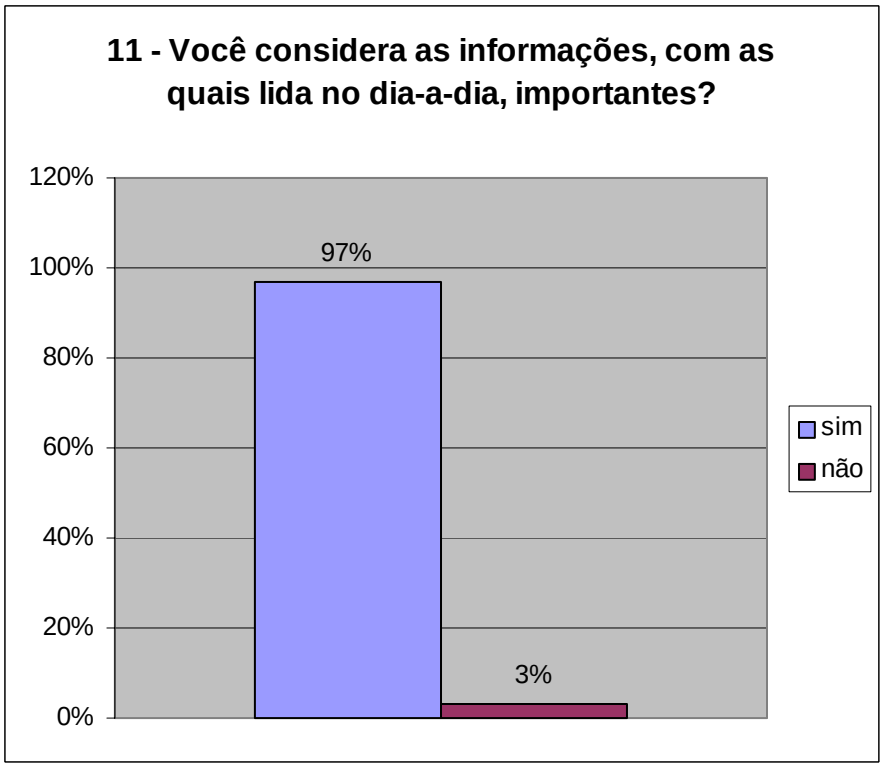


Figura 3.13 – Importância das informações no dia-a-dia

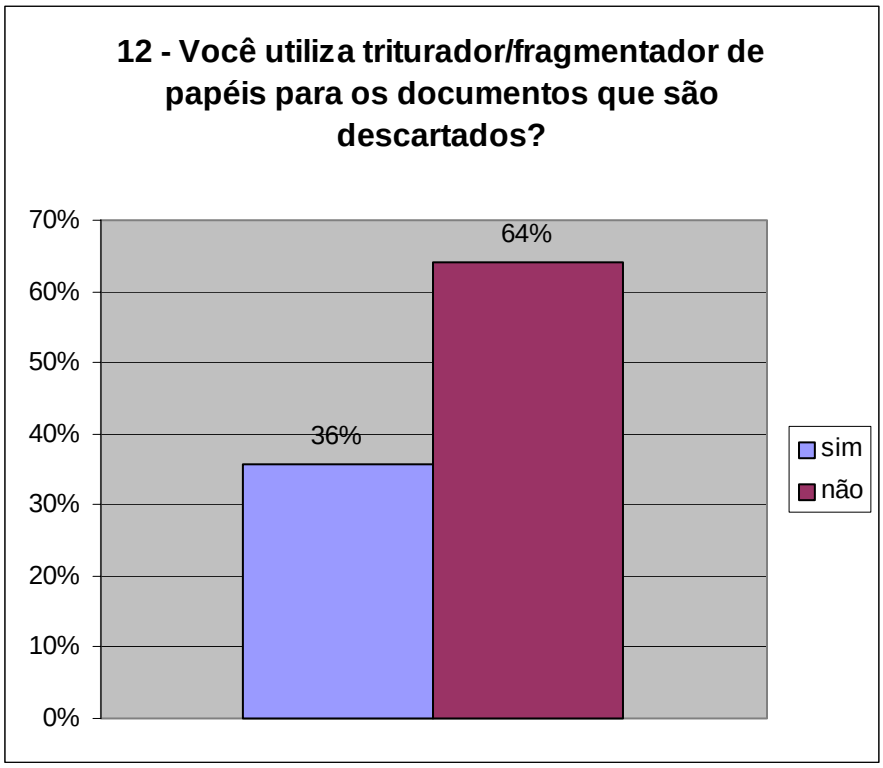


Figura 3.14 – Utilização de triturador/fragmentador de papéis

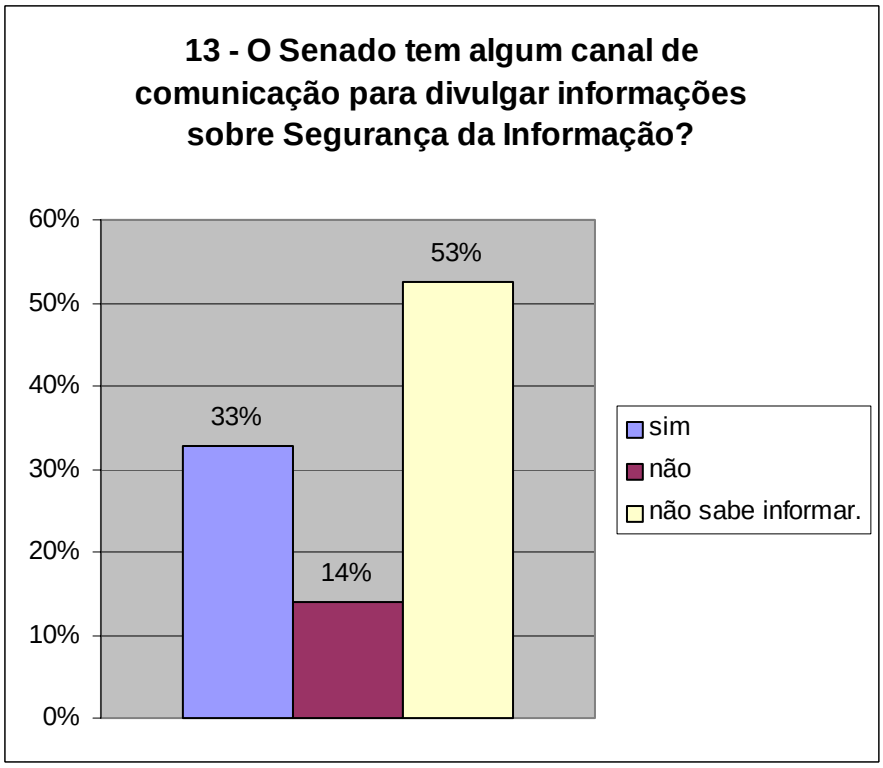


Figura 3.15 – Canal de divulgação sobre Segurança da Informação

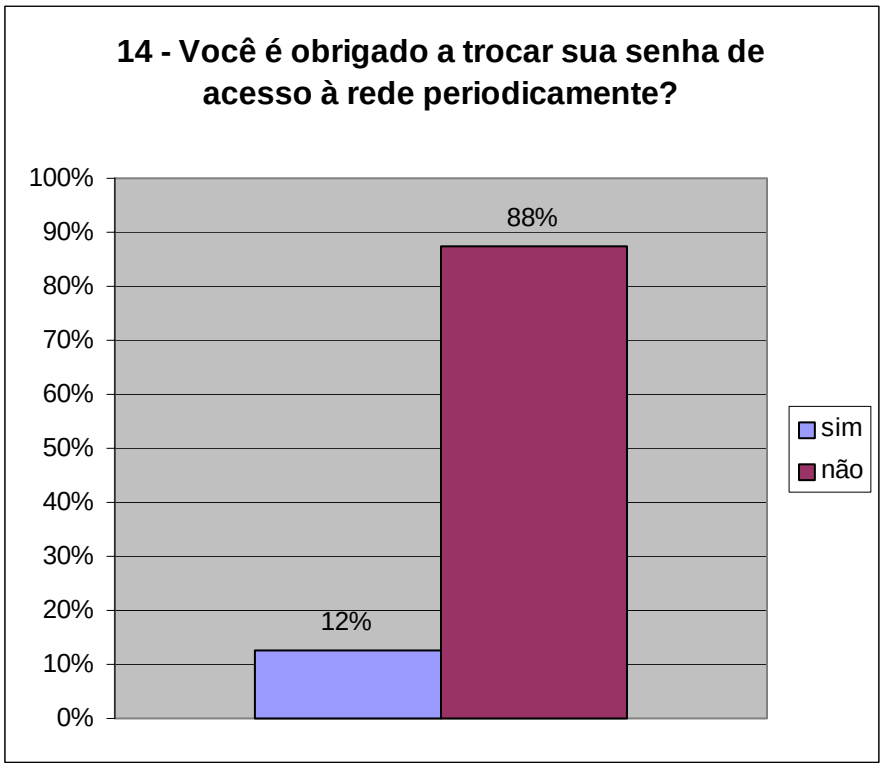


Figura 3.16 – Troca de senha periodicamente

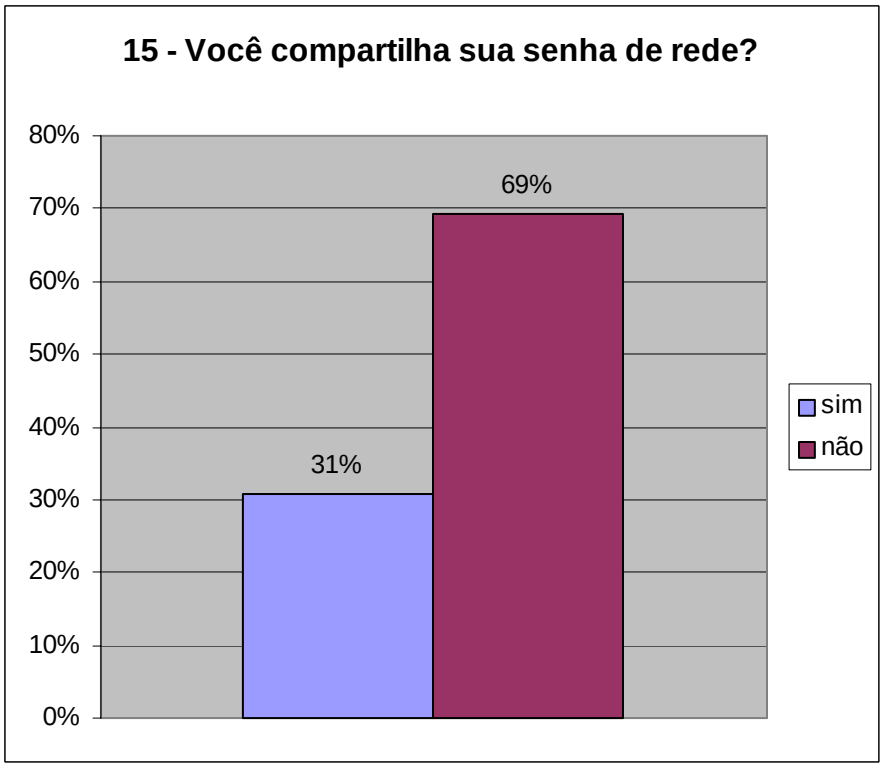


Figura 3.17 – Compartilha senha?

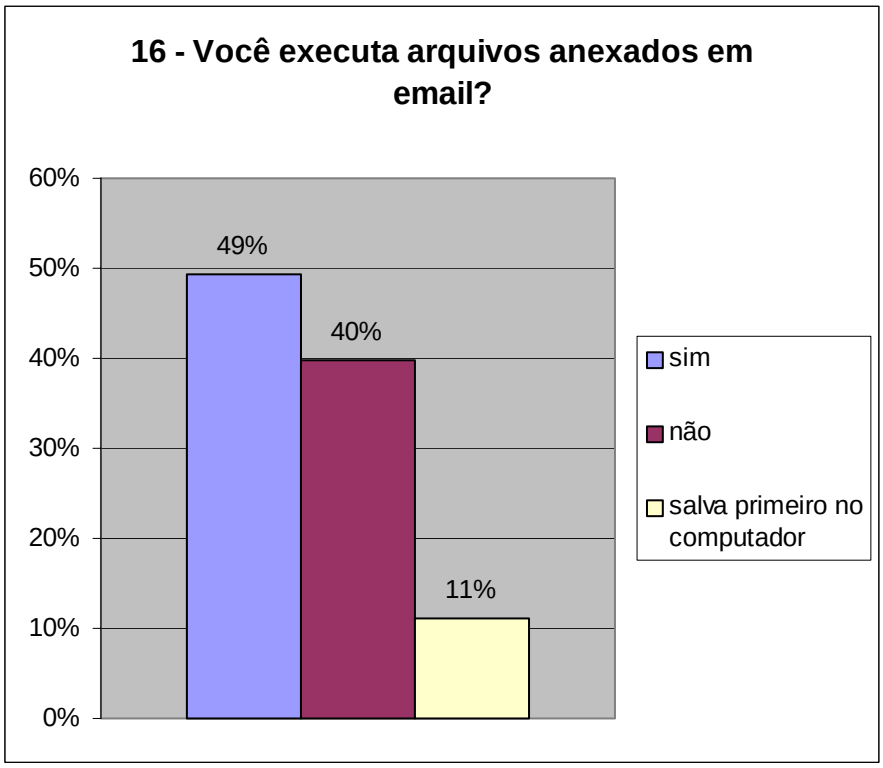


Figura 3.18 – Executa arquivos anexados em e-mail?

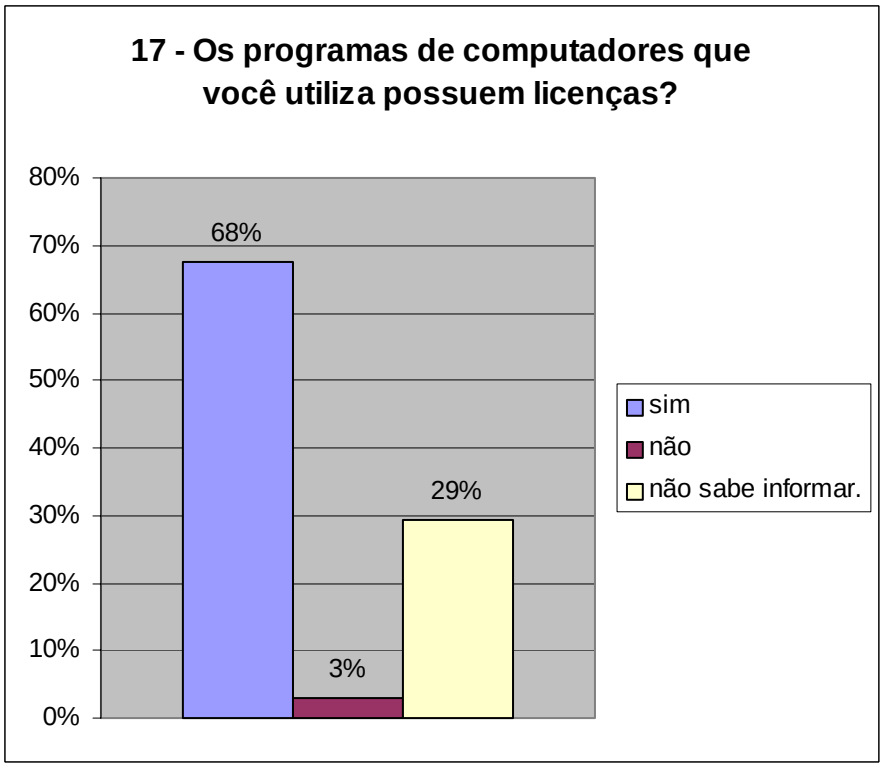


Figura 3.19 – Licenças de softwares

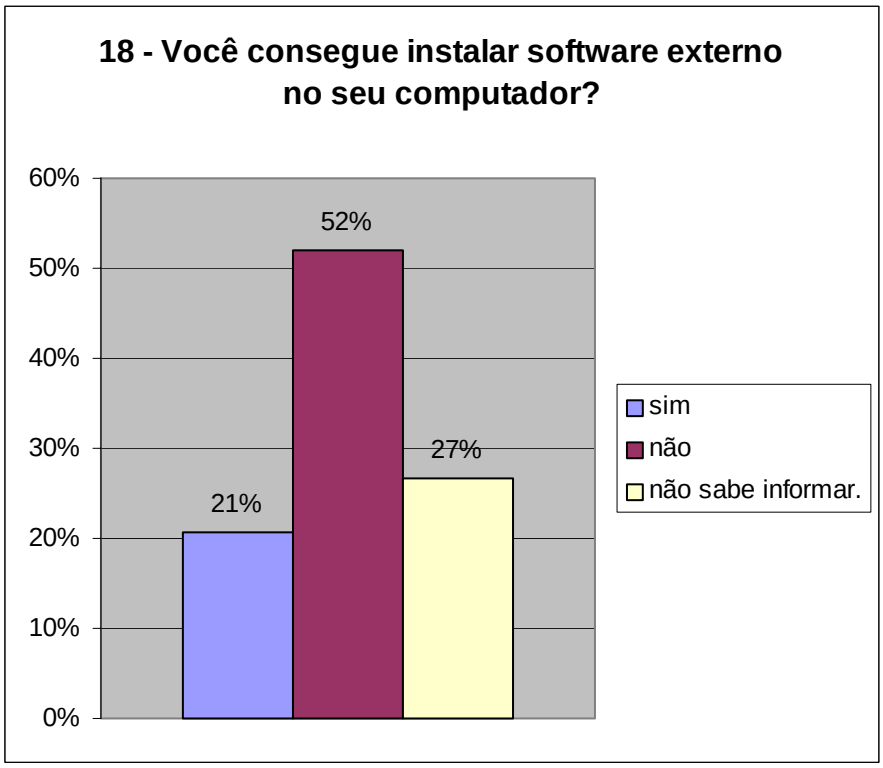


Figura 3.20 – Instalação de *software* externo

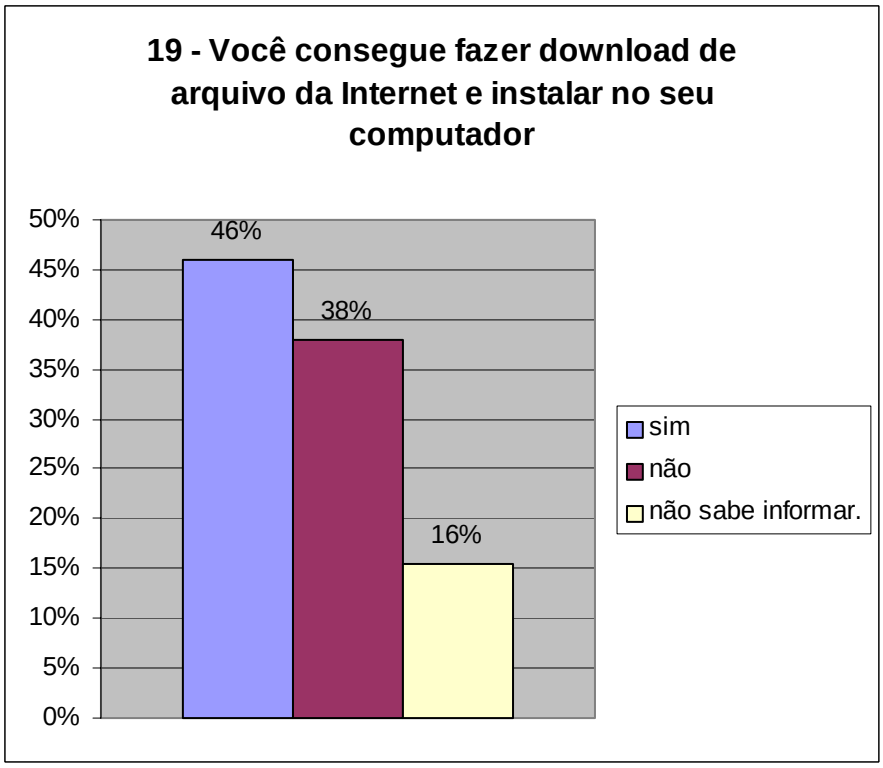


Figura 3.21 – *Download* de arquivo

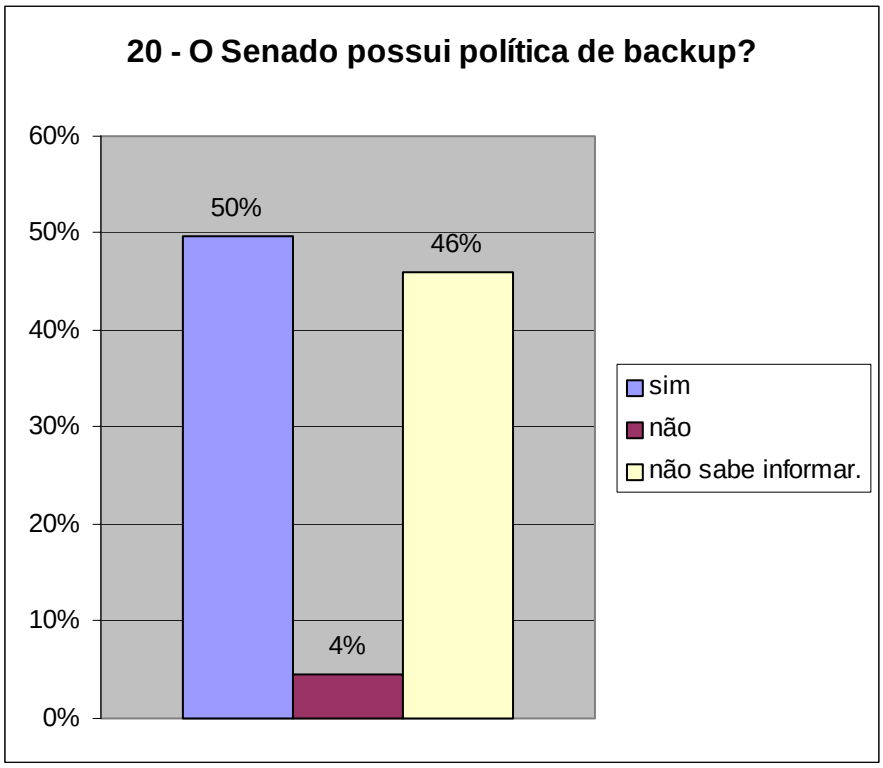


Figura 3.22 – Backup

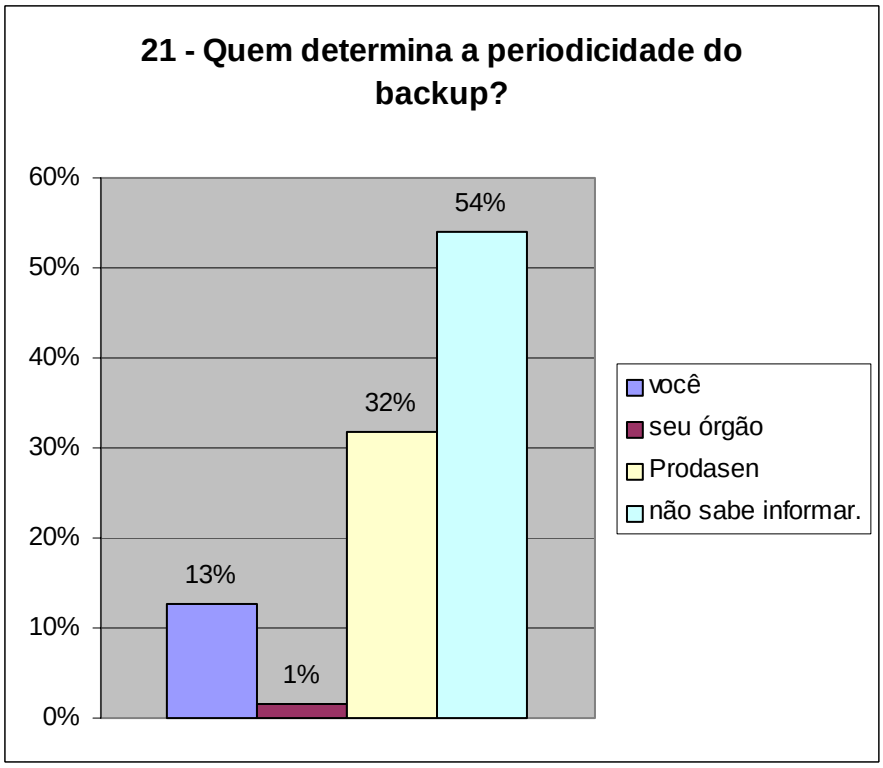


Figura 3.23 – Backup

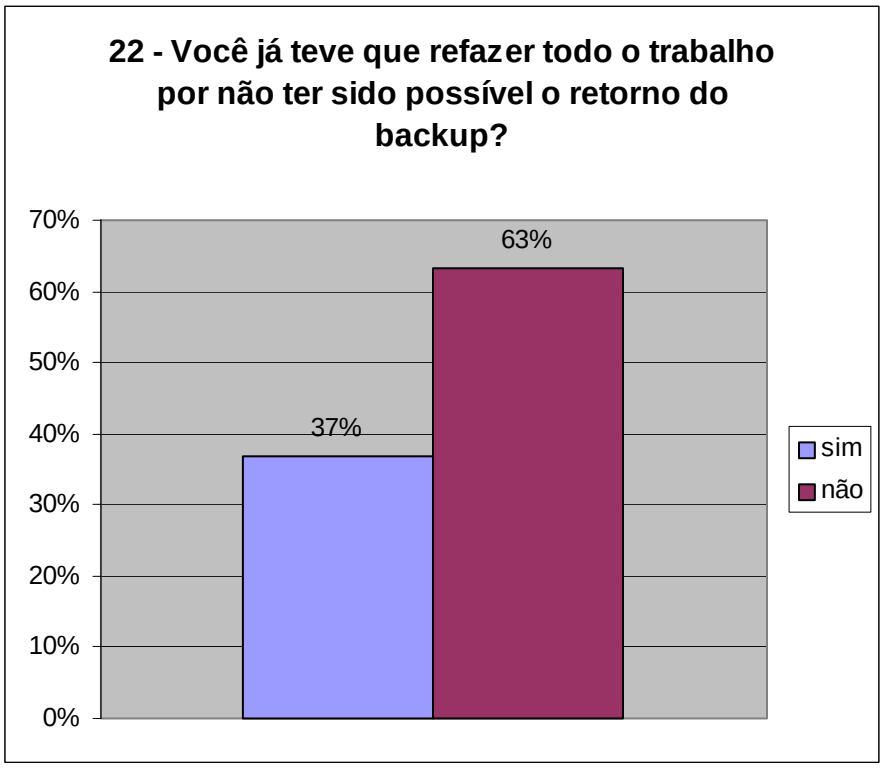


Figura 3.24 – Backup

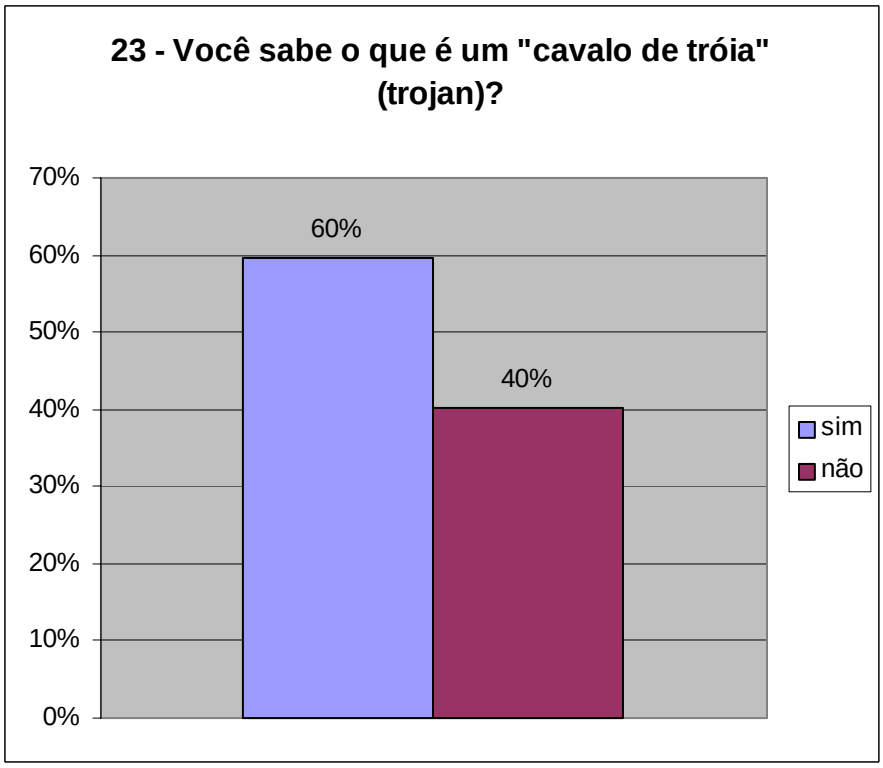


Figura 3.25 – Trojan

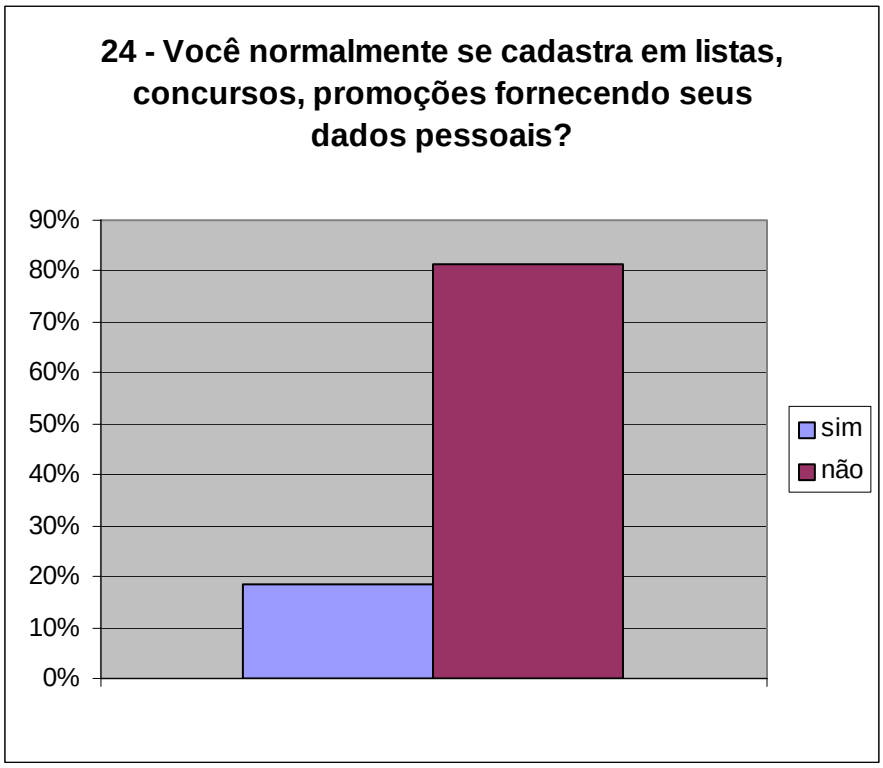


Figura 3.26 – fornecimento de dados pessoais em listas

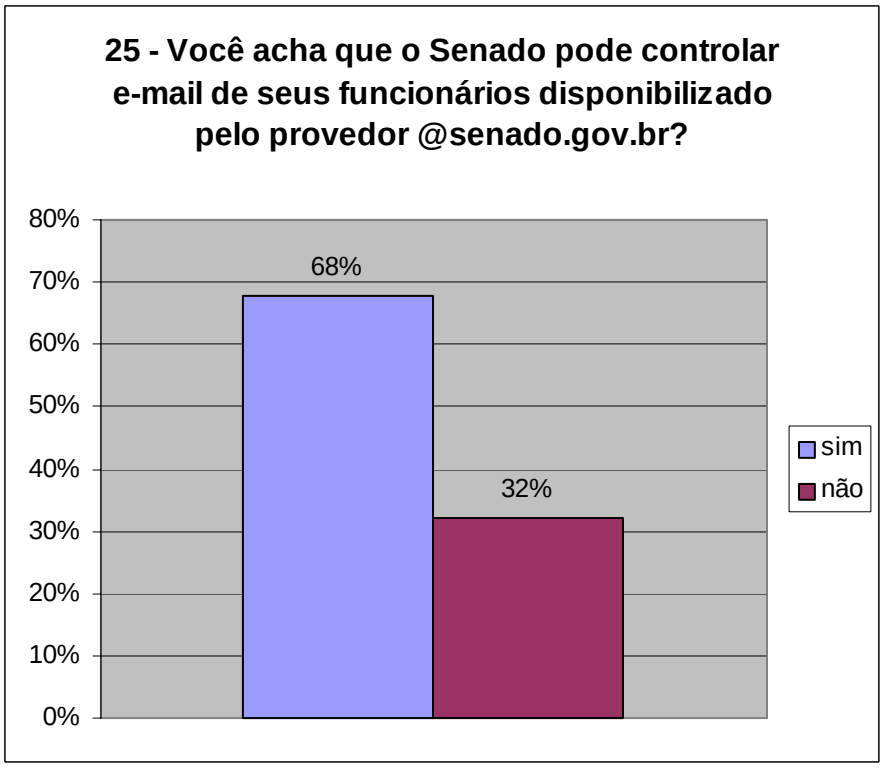


Figura 3.27 – controle de e-mail

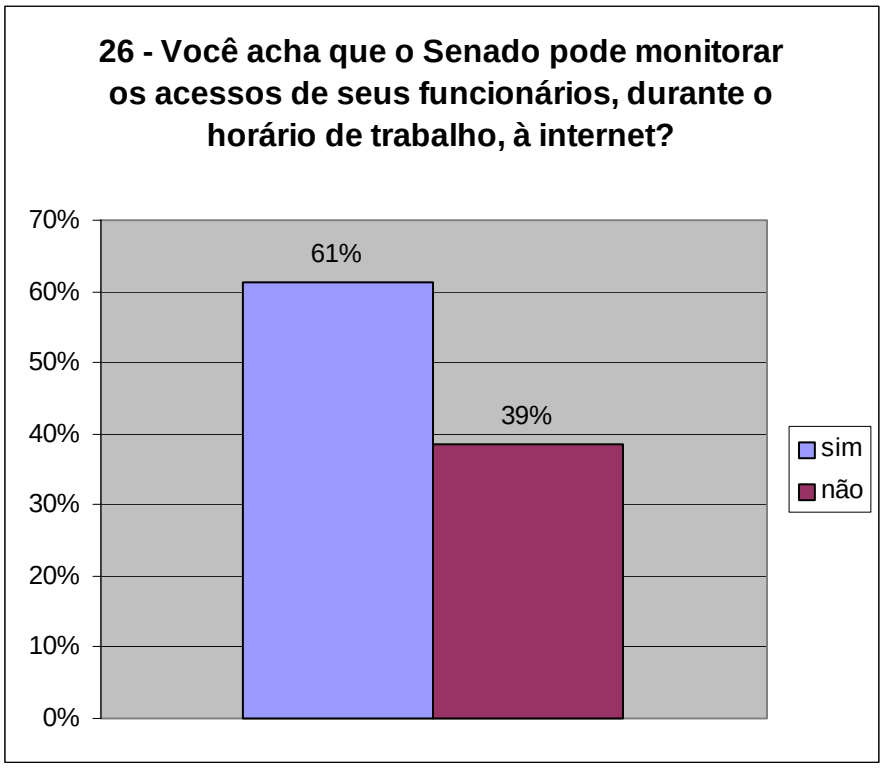


Figura 3.28 – monitoramento de acesso à internet

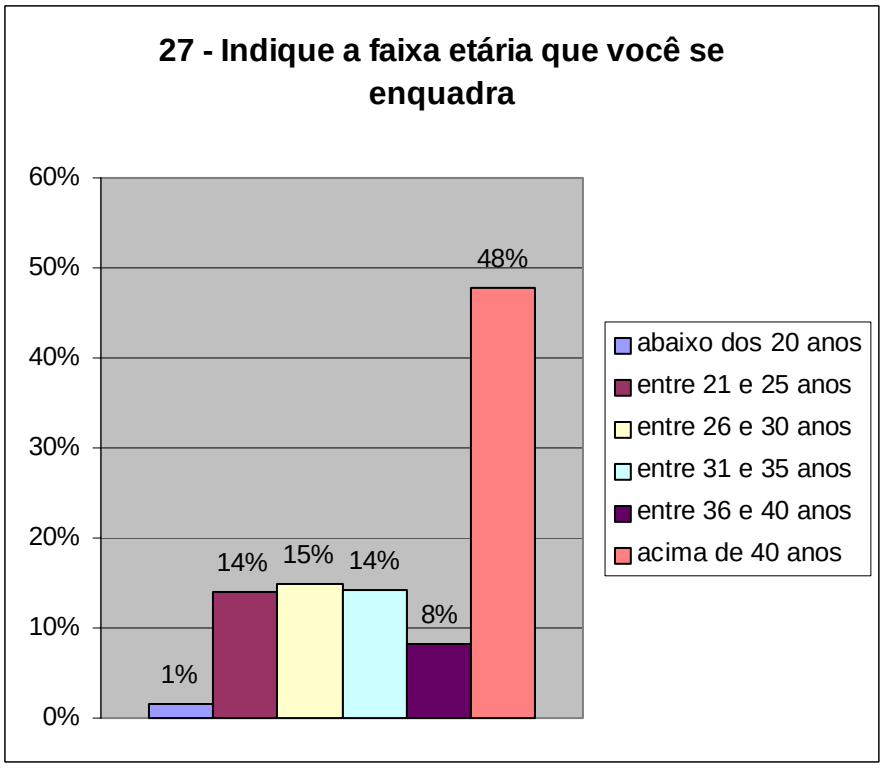


Figura 3.29 – faixa etária

A pesquisa demonstrou que 91% dos entrevistados têm a preocupação com a segurança das informações que utiliza no dia a dia. Porém, 47% não sabem informar se há uma Política de Segurança da Informação no Senado Federal e 84% nunca tiveram treinamento sobre segurança da informação. Apesar de 97% dos entrevistados considerarem suas informações importantes, 69% compartilham sua senha na rede e somente 36% utilizam fragmentador de papel. Outro fato alarmante é que 67% dos usuários já perderam dados por não terem efetuado cópia de segurança ou recuperado do *backup*. Não há por parte da Secretaria Especial de Informática – Prodasen, órgão de TI no Senado, uma política que obrigue os servidores a trocarem suas senhas periodicamente. Esses fatos vêm corroborar que o Senado não possui Política de Segurança da Informação, o que ocasiona um aumento dos riscos e vulnerabilidades na segurança da informação da instituição.

4. REVISÃO DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO

4.1. Leis

As normas relativas a sistemas de informação e segurança da informação no Brasil não estão consolidadas e não há jurisprudência sobre o assunto. Na legislação atual, o crime digital não é considerado uma nova modalidade de crime e sim um crime comum, cuja ferramenta é o computador. Além da consolidação da legislação sobre o assunto, falta preparo pela polícia e pelos legisladores com relação à informática. Com exceção da NBR ISO/IEC 17799:2001 [12], as leis citadas neste capítulo foram anexadas ao final deste trabalho.

No caso específico do Senado Federal, os servidores de efetivos e comissionados são regidos pelo Regime Jurídico Único da Lei nº 8.112, de 1990. Nesta norma não há dispositivos que tratam da obrigação ou proibição quanto a atos praticados pelo funcionário relativos à segurança da informação. Em se tratando de normas internas, não há nenhuma que verse sobre o assunto.

A Lei 9.296/96 é a primeira lei específica para o meio digital. Ela trata basicamente do sigilo das transmissões de dados, segundo a qual é vedado a qualquer pessoa ou entidade o direito de interceptação de mensagens digitais ou telefônicas, bem como quaisquer comunicações entre 2 computadores por meios telefônicos, telemáticos ou digitais.

Em fevereiro de 1998, foi editada a Lei nº 9.608, conhecida como Lei do *Software*, que a define no art. 1º como sendo “a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados". Tais programas receberam a proteção legal contra a cópia ilegal capitulada como crime de sonegação fiscal. A lei dá poderes à Receita Federal para investigar empresas e saber a procedência de programas utilizados nos computadores.

A Lei nº 9.983, de 14 de julho de 2000, acrescentou ao Código Penal artigo Art. 313-A que prevê pena de reclusão de 2 a 12 anos e multa aos funcionários que inserirem dados falsos em sistemas de informações ou bancos de dados da Administração Pública, “com o fim de obter vantagem indevida para sim ou para outrem ou causar dano”. A mesma norma legal

prevê a punição de 3 meses a 2 anos e multa ao funcionário que modificar ou alterar sistemas de informações ou programa de informática sem autorização ou solicitação de autoridade competente. O Art. 2º da referida lei prevê como crime a ação de divulgação de informações sigilosas ou reservadas, contidas ou não nos sistemas de informação ou banco de dados da Administração Pública, com pena de detenção de 1 a 4 anos, e multa.

Em agosto de 2001, por meio da Medida Provisória nº 2.200-2, o governo instituiu a Infra-Estrutura de Chaves Públicas Brasileira – ICP – Brasil, que permitiu o respaldo legal para uso de tecnologia de segurança da informação baseada em certificados digitais. O novo Código Civil (art. 212) diz que uma das modalidades de prova dos fatos jurídicos é a "presunção" A MP 2.200-2 estipula "presunção" legal caso um documento seja assinado digitalmente sob a ICP-Brasil

Duas iniciativas legislativas recentes contribuem para fortificar ainda mais o envio de uma mensagem eletrônica como prova jurídica. O Projeto de Lei 7.316/02, do Instituto de Tecnologia e Informação (ITI), que irá substituir a Medida Provisória 2.200/01, sobre a certificação digital, faz com que documentos assinados eletronicamente ganhem o mesmo valor jurídico de um documento de papel.

Outro projeto de lei, de nº 6.693/06, apresentado pela senadora Sandra Rosado (PSB-RN), também propõe validar as mensagens de correio eletrônico como prova documental.

4.2. Decreto nº 3.505/2000

O Governo Federal legislou a respeito da Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal por meio do Decreto nº 3.505, de 13 de junho de 2000. Essa Política de Segurança visa oferecer instrumentos jurídicos, normativos e organizacionais que capacitem órgão e entidades científica, tecnológica e administrativamente a fim de assegurar a confidencialidade, integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis. Para esta Política, foi criado um Comitê Gestor, composto por representantes de alguns Ministérios e órgãos do Governo para aferir a evolução do assunto. Contudo, decretos se aplicam ao âmbito do Poder Executivo, sendo assim, o Senado Federal não vem aplicando esta norma.

Estas normas visam à redução de riscos e torna-se necessário um conjunto coordenado de trabalhos no país e a nível de Estado, contribuindo para o uso da TI e diminuição dos

riscos advindo da evolução tecnológica, principalmente por empresas e organizações que atuem em áreas consideradas estratégicas e sensíveis ao país.

4.3. NBR ISO/IEC 17799 (2000 e 2005)

Em 1987, o departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (Commercial Computer Security Centre) que dentre suas atribuições tinha a tarefa de criar uma norma de segurança das informações para o Reino Unido. Assim, em 1995 surgiu a Brithish Standart-7799 (BS-7799), norma de segurança da informação destinada a empresas. Esse documento foi disponibilizado em duas partes para consulta pública, a primeira denominada BS-7799-1, em 1995, e a segunda, a BS7799-2, em 1998. A BS7799-1 é a primeira parte da norma que contém uma introdução, definição de extensão e condições principais de uso da norma. Disponibiliza 148 controles divididos em dez partes distintas. É planejada como um documento de referência para implementar "boas práticas" de segurança na empresa. A BS7799-2 é a segunda parte da norma e tem por objetivo proporcionar uma base para gerenciar a segurança da informação dos sistemas das empresas.

Em Abril de 1999 as duas normas (a de 1995 e a de 1998) foram publicadas após uma revisão, com o nome de BS7799-1999; neste período esta norma já estava sendo adotada por outros países, como a Austrália, a África do Sul, a República Checa, a Dinamarca, a Coréia, a Suíça e a Nova Zelândia. BS7799 já foi traduzida para várias línguas entre as quais pode-se destacar o Francês, o Alemão e o Japonês. Neste mesmo ano a primeira parte deste documento foi submetida à "ISO" para homologação, sobre o mecanismo de *Fast Track*. Em maio de 2000 a "BSI" homologou a primeira parte da norma BS7799. Em outubro na reunião do comitê da "ISO" em Tóquio, a norma foi votada e aprovada pela maioria dos representantes. Os representantes dos países ricos, excluindo a Inglaterra, foram todos contra a homologação; mas em primeiro de dezembro de 2000 houve a homologação desta "BS" como "ISO/IEC 17799:2001". Por fim, em setembro de 2001, a ABNT homologou a versão brasileira da norma, denominada NBR ISO/IEC 17799, que é uma tradução literal da norma ISO. Sua publicação inclui oficialmente o Brasil no conjunto de países que, de certa forma, adotam e apóiam o uso da norma de Segurança da Informação.

4.3.1. ISO 27001:2005 [19]

A Norma Britânica BS 7799-2:2002 foi publicada no dia 5 de setembro de 2002. Após um trabalho de cinco anos, que envolveu aproximadamente 100 especialistas em SI de 35 países, foi publicado, em 15 outubro de 2005, a norma ISO 27001:2005, que é a norma BS7799-2:2002 revisada, com melhorias e adaptações contemplando o ciclo PDCA de melhorias e a visão de processos que as normas de sistemas de gestão já incorporaram. Os controles da ISO/IEC 17799 [12] foram adicionados a um anexo desta versão, permitindo uma correspondência entre a numeração em ambas as normas.

O novo padrão agora contém 11 capítulos principais renomeados e reorganizados. Os novos capítulos são:

1. Políticas de Segurança
2. Organizando a Segurança da Informação
3. Gerenciamento de ativos
4. Segurança dos Recursos Humanos
5. Segurança Física e Ambiental
6. Gerenciamento das Comunicações e Operações
7. Controle de Acessos
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
9. Gerenciamento de Incidentes na Segurança da Informação
10. Gerenciamento da Continuidade do Negócio
11. Conformidade.

A nova versão do padrão também introduz controles para tratar de uma série de assuntos antes não considerados. Estes incluem tópicos como o provisionamento para a terceirização (*outsourcing*) e gerência de correções (*patch*). Da mesma forma, outras áreas foram substancialmente estendidas ou re-formatadas, como a rescisão do emprego, e comunicação móvel distribuída.

As principais mudanças foram:

1**)** Tornou a norma *user friendly*, ou seja, de fácil leitura e entendimento. Apresenta o Objetivo do Controle, define qual o Controle a ser implementado e apresenta diretrizes para a sua implementação. Além disso, ainda apresenta informações adicionais, como, por exemplo, aspectos legais e referências a outras normas.

2) Foi criada uma seção específica sobre Análise/Avaliação e tratamento de riscos. Essa seção recomenda que:

a. A análise/avaliação de riscos de SI inclua um enfoque para estimar a magnitude do risco e a comparação contra critérios definidos;

b. As análises/avaliações de riscos de SI periódicas, contemplando as mudanças nos requisitos de SI e na situação de risco;

c.A análise/avaliação de riscos de SI tenha um escopo claramente definido, que pode ser em toda a organização ou em parte dela.

A análise/avaliação de riscos é uma das três fontes principais para que uma Organização identifique os seus requisitos de SI, além de legislações vigentes, estatutos, regulamentações e cláusulas contratuais que a Organização deva atender; e os princípios, objetivos e requisitos do negócio que venha apoiar as operações da Organização.

3) Existe uma nova definição de SI, agora contemplando outras propriedades: autenticidade, não repúdio e confiabilidade. Os componentes principais para a preservação e proteção da informação, como a confidencialidade, a integridade e a disponibilidade, foram mantidos na nova definição.

4) O conceito de ativos foi ampliado para incluir pessoas e imagem/reputação da Organização, além dos ativos de informação, ativos de *software*, ativos físicos e serviços já existentes na versão 2000.

5) Uma nova seção sobre Gestão de Incidentes de SI.

6) Os controles existentes foram atualizados, melhorados e incorporados com outros controles.

7) 17 novos controles foram incorporados na versão 2005.

O próximo passo será a conversão da ISO/EC 17799:2005 em ISO/IEC 27002, previsto para 2007, formando assim a família ISO/IEC 27000 que tratará aspectos mais amplos de Segurança da Informação. No Brasil, a ABNT (Associação Brasileira de Normas Técnicas) lançou no dia 24/08/2005 a versão NBR ISO IEC 17799:2005. A partir de 2007 será numerada como NBR ISO IEC 27002.

4.3.2. Porque Adotar a NBR ISO IEC 17799:2005?

As normas publicadas pela Organização Internacional de Normalização, a ISO, têm uma grande aceitação no mercado. Um exemplo disso é a norma ISO 9001:2000, que trata da Gestão da Qualidade, considerada como a mais difundida norma da ISO que existe no mundo.

No caso da NBR ISO IEC 17799:2005, que é um Código de Boas Práticas para a Segurança da Informação, a sua aplicação é um pouco mais restrita que a ISO 9001:2000, pois ela não é uma norma voltada para fins certificação.

Entretanto, a NBR ISO IEC 17799:2005 pode ser usada pela maioria dos setores da economia, pois todas as organizações, independentemente do seu porte ou do ramo de atuação, do setor público ou privado, precisam proteger as suas informações sensíveis e críticas.

As principais recomendações da NBR ISO IEC 17799 estão detalhadas nas 11 seções abaixo, totalizando 39 categorias principais de SI:

1. Política de Segurança da Informação;
2. Organizando a Segurança da Informação;
3. Gestão de Ativos;
4. Segurança em Recursos Humanos;
5. Segurança Física e do Ambiente;
6. Gerenciamento das Operações e Comunicações;
7. Controle de Acesso;
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
9. Gestão de Incidentes de Segurança da Informação;
10. Gestão da Continuidade de Negócios;
11. Conformidade.

4.3.3. Nova Família das Normas ISO IEC 27000

Como forma de dar suporte à implantação da ISO IEC 27001:2005 [19], o Comitê da ISO IEC que trata da segurança da informação decidiu pela criação de uma família de normas sobre Gestão da Segurança da Informação. Esta família foi batizada pela série ISO IEC 27000, a exemplo da série ISO 9000 das normas de qualidade e da série ISO 14000 das normas sobre meio ambiente.

Esta nova família estará relacionada com os requisitos mandatários da ISO IEC 27001:2005, como, por exemplo, a definição do escopo do Sistema de Gestão da Segurança da Informação, a avaliação de riscos, a identificação de ativos e a eficácia dos controles implementados. Na reunião do Comitê ISO IEC, em Nov/2005 (Kuala Lumpur-Malásia), foram aprovadas as seguintes normas e projetos de norma desta nova família:

Número: ISO IEC NWIP 27000 (NWIP - New Work Item Proposal)

Título: Information Security Management Systems – Fundamentals and Vocabulary

Situação: Ainda nos primeiros estágios de desenvolvimento. Previsão de publicação como norma internacional: 2008/2009.

Aplicação: Apresentar os principais conceitos e modelos de SI.

Número: ISO IEC 27001:2005

Título: Information Security Management Systems - Requirements

Situação: Norma aprovada e publicada pela ISO em 15/10/2005. A ABNT publicará como Norma Brasileira NBR ISO IEC 27001.

Aplicação: A ISO/IEC 27001:2005 é a evolução do padrão britânico BS 7799 Parte 2:2002, que trata da definição de requisitos para um Sistema Gestão de Segurança da Informação. Todas as Organizações; define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um SGSI. Será a base para as Organizações que desejem implantar um SGSI.

Número: ISO IEC 27002:2005 (Atual ISO IEC 17799)

Título: Information Technology – Code of Practice for IS Management

Situação: Norma aprovada e publicada pela ISO em 15/06/2005. No Brasil, a ABNT publicou como Norma Brasileira NBR ISO IEC 17799 no dia 24/08/2005. A partir de 2007, será numerada como NBR ISO IEC 27002.

Aplicação: Guia prático de diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de SI em uma Organização. Os objetivos de controle e os controles atendem aos requisitos identificados na análise/avaliação de riscos.

Número: ISO IEC 1 st WD **27003**

Título: Information Security Management Systems - Implementation Guidance

Situação: Em desenvolvimento, denominado de WD - Working Draft. Previsão de publicação como norma internacional: 2008-2009.

Aplicação: Fornecer um guia prático para implementação de um SGSI, baseado na ISO IEC 27001.

5. CONCLUSÕES

Diante do complexo assunto que envolve a segurança da informação, se pudéssemos sintetizá-la em duas palavras, estas seriam **controle e conscientização**. É com controle que se é possível autorizar ou bloquear pessoas que tentam entrar em ambientes físicos restritos, registrar as tentativas de acesso a sites na Internet, agir com velocidade e eficiência em situações de crise bem como mensurar o prejuízo decorrente da quebra de segurança, inibir de tentativas de ataques, realizar e medir a eficiência de treinamentos de conscientização e capacidade de técnicos e usuários da rede corporativa, etc.

Contudo, um controle eficiente e eficaz só é possível quando há planejamento, implementação, análise e monitoramento das atividades que fazem parte da solução de segurança. O primeiro passo é o planejamento e é fator crítico de sucesso para a iniciativa de gerir a segurança da informação. Outro fator importante é a conscientização do elemento humano da organização quanto a Segurança da Informação. Assim, há que se criar uma Política de Segurança do Senado, com rubrica no orçamento específico para esse fim. Essa política representa a bússola que irá apontar o caminho e os passos que irão formar o mosaico da solução para o Senado Federal.

E quais atividades devem ser implementadas para se criar uma Política de Segurança do Senado Federal? São quatro ações que devem ser tomadas:

1. conscientizar a Alta Direção do Senado da importância da gestão da Segurança da Informação.

2. criar um Comitê de Segurança, posicionado na estrutura do Senado, com autonomia própria e abrangência geral, coordenado por um cargo de direção e composto por representantes de várias áreas do Senado Federal, Secretaria Especial de Informática - Prodasen, Secretaria de Documentação e Informação, Secretaria de Biblioteca, Secretaria de Segurança, Secretaria de Recursos Humanos, Secretaria Especial do Interlegis e Secretaria Especial de Editoração e Publicações. Este comitê deverá ser apoiado por consultoria na área de segurança da informação, serviço este que pode e deve ser prestado por empresa ou pessoa terceirizada, pois esta estará isenta de influências internas e terá melhores condições de avaliar o problema e propor soluções de forma imparcial.

3. após a instituição do Comitê de Segurança, é necessário realizar a avaliação dos riscos para se determinar os requisitos de segurança do Senado Federal. Trata-se de uma tarefa complexa, principalmente por se tratar de uma organização grande e singular que é

o Senado Federal. É imperioso a adoção de uma metodologia que tenha como objetivo a visão consolidada dos processos de negócio, mapeamento de relevância, critérios de importância, estudo de impactos, perímetros e atividades do Senado Federal.

4. elaboração uma Política de Segurança da Informação com base nas Normas ABNT ISO/IEC 17799:2005 [12] e ISO/IEC 27001 [19], que deverá ser divulgada a todos os funcionários e colaboradores do Senado Federal, apoiada por uma massiva campanha de *endomarketing*. O estabelecimento da Política de Segurança da Informação é somente o estágio inicial do processo de mudança de cultura quanto ao tema, sendo assim, a preparação de políticas para o estabelecimento de um ambiente seguro somente se efetiva por meio do comprometimento de seus profissionais e o desenvolvimento de processos que utilizam tecnologias e práticas aderentes a política.

Todos, do funcionário menos graduado até os que ocupam cargos de direção, devem perceber que têm a sua parcela de contribuição. O conteúdo mínimo da Política de Segurança deve contemplar a definição de aspectos gerais da política de forma concisa e objetiva, estabelecendo diretrizes para o desenvolvimento das normas.

Por fim, o sucesso na implementação de uma Política de Segurança está atrelado a uma estratégia que deverá apoiada pela Alta Administração e deverá considerar três aspectos fundamentais: Pessoas, Tecnologia e Processos.

5.1. Dificuldades

A não existência de normas sobre o segurança da informação no Senado Federal, levou o autor a realizar uma pesquisa de opinião entre os funcionários da Casa, estagiários, terceirizados e contratados. Muitas vezes os entrevistados não devolviam o questionário e outros sequer respondiam. O autor também realizou entrevistas a responsáveis por diversos setores da Casa (TI, documentação, gráfica, Interlegis, etc) para saber se havia ou não uma Política de Segurança. Após inúmeros contatos, chegou-se a conclusão de que cada Secretaria e seus serviços utilizam uma metodologia de segurança própria, contudo não foi possível obter o documento por escrito dessas práticas.

5.2. Trabalhos Futuros

Esse trabalho será submetido ao Diretor da Secretaria de Recursos Humanos do Senado Federal para avaliação das propostas aqui apresentadas e se aprovado, poderá ser apresentado à Alta Administração da Casa.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] SÊMOLA, M. **Gestão da Segurança da Informação, Uma visão executiva**. 7. ed. Rio de Janeiro: Elsevier, 2003.

[2] Diretoria de Auditoria da Tecnologia da Informação do Tribunal de Contas da União. **Boas Práticas em Segurança da Informação**. Brasília, 2003. 73 p.

[3] FERREIRA, F. N. F.; ARAÚJO, M. T. **Política da Segurança da Informação: Guia Prático para Elaboração e Implementação**. 1. ed. Rio de Janeiro: Ciência Moderna, 2006.

[4] GATES, B. **A Empresa na Velocidade do Pensamento**. Companhia das Letras, 1998. 448 p.

[5] PEREIRA C. **Atividades de Gestão da Segurança da Informação**. Disponível em http://www.trueaccess.com.br/downl_artigos/artigo%20-%20atividades%20da%20gestao%20corporativa%20de%20seguranca.pdf. Acessado em 28-4-2006.

[6] Foco Security. **Análise de Risco**. Disponível em http://www.focosecurity.com.br/. Acessado em 21-06-2006.

[7] MOITA, E. S.; SOUZA, L. A., **A Previdência Social e o Gerenciamento de Risco**s. Disponível em http://www.previdencia.gov.br. Acessado em 26-06-2006.

[8] BETANHO, Cristiane. **Gestão de riscos**: uma abordagem da empresa pública desaneamento. Relatório Reflexivo. Mestrado Integrado em Administração. Universidade São Francisco, 2002.

[9] FERREIRA, F. N. F. **Segurança da Informação**. Editora Ciência Moderna: Rio de Janeiro, 2003.

[10] PEIXOTO, Mário César Pintaudi **Engenharia Social e Segurança da Informação**. Ed. Brasport: Rio de Janeiro, 2006.

[11] **O Jogo da Segurança: descubra as ameaças e vulnerabilidades em ambiente corporativo**. Módulo Security Magazine, São Paulo, nº 345, 2004. Disponível em http://www.modulo.com.br/arquivoboletins/2k4/msnews_no345.htm. Acesso em 2-5-2006

[12] ABNT. NBR ISO/IEC 17799 - **Tecnologia da informação: código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2001.

[13] PINHEIRO, J. M. S. **Biometria na Segurança de Redes de Computadores.** Nov. 2004. Disponível em http://www.projetoderedes.com.br/artigos/artigo_biometria_na_seguranca_das_redes.php. Acesso em 29-6-2006.

[14] HARGER, Vera P. **Princípios de Segurança da Informação**. Apostila ministrada no Curso de Gestão de Tecnologia da Informação da Unilegis. Maio de 2006.

[15] FRISCH, A. **Essential System Administration**, 2nd Edition. Oreilly. 1995.

[16] ALECRIM, E. "**Fique Atento: Scams Usam Sustos para Enganar Internautas**". Disponível em http://www.infowester.com/col200305.php. Acessado em 19-06-2006.

[17] MITNICK, K. ; WILLIAM L. **A arte de enganar**: ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

[18] ALECRIM, E. **Ataques da Engenharia Social na Internet**. Disponível em http://www.infowester.com/col120904.php . Acessado em 16-06-2006.

[19] ABNT. NBR ISSO/IEC 27001 – **Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação** – Requisitos. Rio de Janeiro. ABNT, 2006.

GLOSSÁRIO

business-to-business (B2B)	Negócios para empresas de negócios É o uso de uma rede, em especial a Internet para a comercialização entre empresas que nesta modalidade, comercializam seus produtos e serviços.
business-to-consumer (B2C)	*Business to consumer* é o segmento dentro do comércio eletrônico que abrange qualquer transação em que uma companhia ou organização vende seus produtos ou serviços para as pessoas que navegam pela *Internet*.
business-to-government (B2G)	é o segmento dentro do comércio eletrônico que abrange qualquer transação entre empresas e governo
e-comerce	capacidade de realizar transações envolvendo a troca de bens ou serviços entre duas ou mais partes utilizando meios eletrônicos.
ERP	*Enterprise Resources Planning* ou Planejamento de Recursos Empresariais, são uma plataforma de *software* desenvolvida para integrar os diversos departamentos de uma empresa, possibilitando a automação e armazenamento de todas as informações de negócio.

ANEXOS

LEI Nº 9.296, DE 24 DE JULHO DE 1996

Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal;

II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:

I - da autoridade policial, na investigação criminal;

II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.

Art. 4° O pedido de interceptação de comunicação telefônica conterá a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados.

§ 1° Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a interceptação, caso em que a concessão será condicionada à sua redução a termo.

§ 2° O juiz, no prazo máximo de vinte e quatro horas, decidirá sobre o pedido.

Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova.

Art. 6° Deferido o pedido, a autoridade policial conduzirá os procedimentos de interceptação, dando ciência ao Ministério Público, que poderá acompanhar a sua realização.

§ 1° No caso de a diligência possibilitar a gravação da comunicação interceptada, será determinada a sua transcrição.

§ 2° Cumprida a diligência, a autoridade policial encaminhará o resultado da interceptação ao juiz, acompanhado de auto circunstanciado, que deverá conter o resumo das operações realizadas.

§ 3° Recebidos esses elementos, o juiz determinará a providência do art. 8° , ciente o Ministério Público.

Art. 7° Para os procedimentos de interceptação de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.

Art. 8° A interceptação de comunicação telefônica, de qualquer natureza, ocorrerá em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, preservando-se o sigilo das diligências, gravações e transcrições respectivas.

Parágrafo único. A apensação somente poderá ser realizada imediatamente antes do relatório da autoridade, quando se tratar de inquérito policial (Código de Processo Penal, art.10, § 1°) ou na conclusão do processo ao juiz para o despacho decorrente do disposto nos arts. 407, 502 ou 538 do Código de Processo Penal.

Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.

Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.

Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena: reclusão, de dois a quatro anos, e multa.

Art. 11. Esta Lei entra em vigor na data de sua publicação.

Art. 12. Revogam-se as disposições em contrário.

Brasília, 24 de julho de 1996; 175º da Independência e 108º da República.

FERNANDO HENRIQUE CARDOSO

Nelson A. Jobim

LEI Nº 9.609 , DE 19 DE FEVEREIRO DE 1998

Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

CAPÍTULO II

DA PROTEÇÃO AOS DIREITOS DE AUTOR E DO REGISTRO

Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.

§ 1º Não se aplicam ao programa de computador as disposições relativas aos direitos morais, ressalvado, a qualquer tempo, o direito do autor de reivindicar a paternidade do programa de computador e o direito do autor de opor-se a alterações não-autorizadas, quando estas impliquem deformação, mutilação ou outra modificação do programa de computador, que prejudiquem a sua honra ou a sua reputação.

§ 2º Fica assegurada a tutela dos direitos relativos a programa de computador pelo prazo de cinqüenta anos, contados a partir de 1º de janeiro do ano subseqüente ao da sua publicação ou, na ausência desta, da sua criação.

§ 3º A proteção aos direitos de que trata esta Lei independe de registro.

§ 4º Os direitos atribuídos por esta Lei ficam assegurados aos estrangeiros domiciliados no exterior, desde que o país de origem do programa conceda, aos brasileiros e estrangeiros domiciliados no Brasil, direitos equivalentes.

§ 5º Inclui-se dentre os direitos assegurados por esta Lei e pela legislação de direitos autorais e conexos vigentes no País aquele direito exclusivo de autorizar ou proibir o aluguel comercial, não sendo esse direito exaurível pela venda, licença ou outra forma de transferência da cópia do programa.

§ 6º O disposto no parágrafo anterior não se aplica aos casos em que o programa em si não seja objeto essencial do aluguel.

Art. 3º Os programas de computador poderão, a critério do titular, ser registrados em órgão ou entidade a ser designado por ato do Poder Executivo, por iniciativa do Ministério responsável pela política de ciência e tecnologia.

§ 1º O pedido de registro estabelecido neste artigo deverá conter, pelo menos, as seguintes informações:

I - os dados referentes ao autor do programa de computador e ao titular, se distinto do autor, sejam pessoas físicas ou jurídicas;

II - a identificação e descrição funcional do programa de computador; e

III - os trechos do programa e outros dados que se considerar suficientes para identificá-lo e caracterizar sua originalidade, ressalvando-se os direitos de terceiros e a responsabilidade do Governo.

§ 2º As informações referidas no inciso III do parágrafo anterior são de caráter sigiloso, não podendo ser reveladas, salvo por ordem judicial ou a requerimento do próprio titular.

Art. 4º Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos.

§ 1º Ressalvado ajuste em contrário, a compensação do trabalho ou serviço prestado limitar-se-á à remuneração ou ao salário convencionado.

§ 2º Pertencerão, com exclusividade, ao empregado, contratado de serviço ou servidor os direitos concernentes a programa de computador gerado sem relação com o contrato de trabalho, prestação de serviços ou vínculo estatutário, e sem a utilização de recursos, informações tecnológicas, segredos industriais e de negócios, materiais, instalações ou equipamentos do empregador, da empresa ou entidade com a qual o empregador mantenha contrato de prestação de serviços ou assemelhados, do contratante de serviços ou órgão público.

§ 3º O tratamento previsto neste artigo será aplicado nos casos em que o programa de computador for desenvolvido por bolsistas, estagiários e assemelhados.

Art. 5º Os direitos sobre as derivações autorizadas pelo titular dos direitos de programa de computador, inclusive sua exploração econômica, pertencerão à pessoa autorizada que as fizer, salvo estipulação contratual em contrário.

Art. 6º Não constituem ofensa aos direitos do titular de programa de computador:

I - a reprodução, em um só exemplar, de cópia legitimamente adquirida, desde que se destine à cópia de salvaguarda ou armazenamento eletrônico, hipótese em que o exemplar original servirá de salvaguarda;

II - a citação parcial do programa, para fins didáticos, desde que identificados o programa e o titular dos direitos respectivos;

III - a ocorrência de semelhança de programa a outro, preexistente, quando se der por força das características funcionais de sua aplicação, da observância de preceitos normativos e técnicos, ou de limitação de forma alternativa para a sua expressão;

IV - a integração de um programa, mantendo-se suas características essenciais, a um sistema aplicativo ou operacional, tecnicamente indispensável às necessidades do usuário, desde que para o uso exclusivo de quem a promoveu.

CAPÍTULO III

DAS GARANTIAS AOS USUÁRIOS DE PROGRAMA DE COMPUTADOR

Art. 7º O contrato de licença de uso de programa de computador, o documento fiscal correspondente, os suportes físicos do programa ou as respectivas embalagens deverão consignar, de forma facilmente legível pelo usuário, o prazo de validade técnica da versão comercializada.

Art. 8º Aquele que comercializar programa de computador, quer seja titular dos direitos do programa, quer seja titular dos direitos de comercialização, fica obrigado, no território nacional, durante o prazo de validade técnica da respectiva versão, a assegurar aos respectivos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento do programa, consideradas as suas especificações.

Parágrafo único. A obrigação persistirá no caso de retirada de circulação comercial do programa de computador durante o prazo de validade, salvo justa indenização de eventuais prejuízos causados a terceiros.

CAPÍTULO IV

DOS CONTRATOS DE LICENÇA DE USO, DE COMERCIALIZAÇÃO E DE TRANSFERÊNCIA DE TECNOLOGIA

Art. 9º O uso de programa de computador no País será objeto de contrato de licença.

Parágrafo único. Na hipótese de eventual inexistência do contrato referido no *caput* deste artigo, o documento fiscal relativo à aquisição ou licenciamento de cópia servirá para comprovação da regularidade do seu uso.

Art. 10. Os atos e contratos de licença de direitos de comercialização referentes a programas de computador de origem externa deverão fixar, quanto aos tributos e encargos exigíveis, a responsabilidade pelos respectivos pagamentos e estabelecerão a remuneração do titular dos direitos de programa de computador residente ou domiciliado no exterior.

§ 1º Serão nulas as cláusulas que:

I - limitem a produção, a distribuição ou a comercialização, em violação às disposições normativas em vigor;

II - eximam qualquer dos contratantes das responsabilidades por eventuais ações de terceiros, decorrentes de vícios, defeitos ou violação de direitos de autor.

§ 2º O remetente do correspondente valor em moeda estrangeira, em pagamento da remuneração de que se trata, conservará em seu poder, pelo prazo de cinco anos, todos os documentos necessários à comprovação da licitude das remessas e da sua conformidade ao *caput* deste artigo.

Art. 11. Nos casos de transferência de tecnologia de programa de computador, o Instituto Nacional da Propriedade Industrial fará o registro dos respectivos contratos, para que produzam efeitos em relação a terceiros.

Parágrafo único. Para o registro de que trata este artigo, é obrigatória a entrega, por parte do fornecedor ao receptor de tecnologia, da documentação completa, em especial do código-fonte comentado, memorial descritivo, especificações funcionais internas, diagramas, fluxogramas e outros dados técnicos necessários à absorção da tecnologia.

CAPÍTULO V

DAS INFRAÇÕES E DAS PENALIDADES

Art. 12. Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;

II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Art. 13. A ação penal e as diligências preliminares de busca e apreensão, nos casos de violação de direito de autor de programa de computador, serão precedidas de vistoria, podendo o juiz ordenar a apreensão das cópias produzidas ou comercializadas com violação de direito de autor, suas versões e derivações, em poder do infrator ou de quem as esteja expondo, mantendo em depósito, reproduzindo ou comercializando.

Art. 14. Independentemente da ação penal, o prejudicado poderá intentar ação para proibir ao infrator a prática do ato incriminado, com cominação de pena pecuniária para o caso de transgressão do preceito.

§ 1º A ação de abstenção de prática de ato poderá ser cumulada com a de perdas e danos pelos prejuízos decorrentes da infração.

§ 2º Independentemente de ação cautelar preparatória, o juiz poderá conceder medida liminar proibindo ao infrator a prática do ato incriminado, nos termos deste artigo.

§ 3º Nos procedimentos cíveis, as medidas cautelares de busca e apreensão observarão o disposto no artigo anterior.

§ 4º Na hipótese de serem apresentadas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.

§ 5º Será responsabilizado por perdas e danos aquele que requerer e promover as medidas previstas neste e nos arts. 12 e 13, agindo de má-fé ou por espírito de emulação, capricho ou erro grosseiro, nos termos dos arts. 16, 17 e 18 do Código de Processo Civil.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 15. Esta Lei entra em vigor na data de sua publicação.

Art. 16. Fica revogada a Lei nº 7.646, de 18 de dezembro de 1987.

Brasília, 19 de fevereiro de 1998; 177º da Independência e 110º da República.

FERNANDO HENRIQUE CARDOSO

José Israel Vargas

Lei nº 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.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º São acrescidos à Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, os seguintes dispositivos:

"Apropriação indébita previdenciária"

"Art. 168-A. Deixar de repassar à previdência social as contribuições recolhidas dos contribuintes, no prazo e forma legal ou convencional:"

"Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa."

"§ 1º Nas mesmas penas incorre quem deixar de:"

"I – recolher, no prazo legal, contribuição ou outra importância destinada à previdência social que tenha sido descontada de pagamento efetuado a segurados, a terceiros ou arrecadada do público;"

"II – recolher contribuições devidas à previdência social que tenham integrado despesas contábeis ou custos relativos à venda de produtos ou à prestação de serviços;"

"III - pagar benefício devido a segurado, quando as respectivas cotas ou valores já tiverem sido reembolsados à empresa pela previdência social."

"§ 2º É extinta a punibilidade se o agente, espontaneamente, declara, confessa e efetua o pagamento das contribuições, importâncias ou valores e presta as informações devidas à previdência social, na forma definida em lei ou regulamento, antes do início da ação fiscal."

"§ 3º É facultado ao juiz deixar de aplicar a pena ou aplicar somente a de multa se o agente for primário e de bons antecedentes, desde que:"

"I – tenha promovido, após o início da ação fiscal e antes de oferecida a denúncia, o pagamento da contribuição social previdenciária, inclusive acessórios; ou"

"II – o valor das contribuições devidas, inclusive acessórios, seja igual ou inferior àquele estabelecido pela previdência social, administrativamente, como sendo o mínimo para o ajuizamento de suas execuções fiscais."

"Inserção de dados falsos em sistema de informações"

"Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:"

"Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa."

"Modificação ou alteração não autorizada

de sistema de informações"

"Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:"

"Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa."

"Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado."

"Sonegação de contribuição previdenciária"

"Art. 337-A. Suprimir ou reduzir contribuição social previdenciária e qualquer acessório, mediante as seguintes condutas:"

"I – omitir de folha de pagamento da empresa ou de documento de informações previsto pela legislação previdenciária segurados empregado, empresário, trabalhador avulso ou trabalhador autônomo ou a este equiparado que lhe prestem serviços;"

"II – deixar de lançar mensalmente nos títulos próprios da contabilidade da empresa as quantias descontadas dos segurados ou as devidas pelo empregador ou pelo tomador de serviços;"

"III – omitir, total ou parcialmente, receitas ou lucros auferidos, remunerações pagas ou creditadas e demais fatos geradores de contribuições sociais previdenciárias:"

"Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa."

"§ 1º É extinta a punibilidade se o agente, espontaneamente, declara e confessa as contribuições, importâncias ou valores e presta as informações devidas à previdência social, na forma definida em lei ou regulamento, antes do início da ação fiscal."

"§ 2º É facultado ao juiz deixar de aplicar a pena ou aplicar somente a de multa se o agente for primário e de bons antecedentes, desde que:"

"I – (VETADO)"

"II – o valor das contribuições devidas, inclusive acessórios, seja igual ou inferior àquele estabelecido pela previdência social, administrativamente, como sendo o mínimo para o ajuizamento de suas execuções fiscais."

"§ 3º Se o empregador não é pessoa jurídica e sua folha de pagamento mensal não ultrapassa R$ 1.510,00 (um mil, quinhentos e dez reais), o juiz poderá reduzir a pena de um terço até a metade ou aplicar apenas a de multa."

"§ 4º O valor a que se refere o parágrafo anterior será reajustado nas mesmas datas e nos mesmos índices do reajuste dos benefícios da previdência social."

Art. 2º Os arts. 153, 296, 297, 325 e 327 do Decreto-Lei Nº 2.848, de 1940, passam a vigorar com as seguintes alterações:

"Art. 153. ....."

"§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:"

"Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa."

"§ 1º (parágrafo único original)....."

"§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada."

"Art. 296. ....."

"§ 1º .....

....."

"III – quem altera, falsifica ou faz uso indevido de marcas, logotipos, siglas ou quaisquer outros símbolos utilizados ou identificadores de órgãos ou entidades da Administração Pública."

"....."

"Art. 297. .....

....."

"§ 3º Nas mesmas penas incorre quem insere ou faz inserir:"

"I – na folha de pagamento ou em documento de informações que seja destinado a fazer prova perante a previdência social, pessoa que não possua a qualidade de segurado obrigatório;"

"II – na Carteira de Trabalho e Previdência Social do empregado ou em documento que deva produzir efeito perante a previdência social, declaração falsa ou diversa da que deveria ter sido escrita;"

"III – em documento contábil ou em qualquer outro documento relacionado com as obrigações da empresa perante a previdência social, declaração falsa ou diversa da que deveria ter constado."

"§ 4º Nas mesmas penas incorre quem omite, nos documentos mencionados no § 3º, nome do segurado e seus dados pessoais, a remuneração, a vigência do contrato de trabalho ou de prestação de serviços."

"Art. 325. ....."

"§ 1º Nas mesmas penas deste artigo incorre quem:"

"I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;"

"II – se utiliza, indevidamente, do acesso restrito."

"§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:"

"Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa."

"Art. 327. ....."

"§ 1º Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública." (NR)

"....."

Art. 3º O art. 95 da Lei Nº 8.212, de 24 de julho de 1991, passa a vigorar com a seguinte redação:

"Art. 95. Caput. Revogado."

"a) revogada;"
"b) revogada;"
"c) revogada;"
"d) revogada;"
"e) revogada;"
"f) revogada;"
"g) revogada;"
"h) revogada;"
"i) revogada;"
"j) revogada."
"§ 1º Revogado."
"§ 2º ....."
"a) ....."
"b) ....."
"c) ....."
"d) ....."
"e)....."
"f)....."
"§ 3º Revogado."
"§ 4º Revogado."
"§ 5º Revogado."

Art. 4º Esta Lei entra em vigor noventa dias após a data de sua publicação.

Brasília, 14 de julho de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Waldeck Ornelas

Publicada no DOU de 17/07/2000

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62º da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência

da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais

prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar,

quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários

na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados

como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de

acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10º Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil,

desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11º A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei no 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12º Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13º O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14º No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15º Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16º Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17º Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação

do Ministério da Ciência e Tecnologia; e

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei no 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18º Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia

Geral da União.

Art. 19º Ficam convalidados os atos praticados com base na Medida Provisória no 2.200-1, de 27 de julho de 2001.

Art. 20º Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO

José Gregori Martus Tavares

Ronaldo Mota Sardenberg Pedro Parente

DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000

Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso IV, da Constituição, e tendo em vista o disposto na Lei nº 8.159, de 8 de janeiro de 1991, e no Decreto nº 2.910, de 29 de dezembro de 1998, **D E C R E T A :**

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:

I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;

II - proteção de assuntos que mereçam tratamento especial;

III - capacitação dos segmentos das tecnologias sensíveis;

IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;

V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;

VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e

VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:

I - Certificado de Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal;

II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Art. 3º São objetivos da Política da Informação:

I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

IV - estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;

V - promover as ações necessárias à implementação e manutenção da segurança da informação;

VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;

VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e

VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação.

Art. 4º Para os fins deste Decreto, cabe à Secretaria-Executiva do Conselho de Defesa Nacional, assessorada pelo Comitê Gestor da Segurança da Informação de que trata o art. 6o, adotar as seguintes diretrizes:

I - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos de que trata o artigo anterior, visando garantir a adequada articulação entre os órgãos e as entidades da Administração Pública Federal;

II - estabelecer programas destinados à formação e ao aprimoramento dos recursos humanos, com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer as equipes de pesquisa e desenvolvimento, especializadas em todos os campos da segurança da informação;

III - propor regulamentação sobre matérias afetas à segurança da informação nos órgãos e nas entidades da Administração Pública Federal;

IV - estabelecer normas relativas à implementação da Política Nacional de Telecomunicações, inclusive sobre os serviços prestados em telecomunicações, para assegurar, de modo alternativo, a permanente disponibilização dos dados e das informações de interesse para a defesa nacional;

V - acompanhar, em âmbito nacional e internacional, a evolução doutrinária e tecnológica das atividades inerentes à segurança da informação;

VI - orientar a condução da Política de Segurança da Informação já existente ou a ser implementada;

VII - realizar auditoria nos órgãos e nas entidades da Administração Pública Federal, envolvidas com a política de segurança da informação, no intuito de aferir o nível de segurança dos respectivos sistemas de informação;

VIII - estabelecer normas, padrões, níveis, tipos e demais aspectos relacionados ao emprego dos produtos que incorporem recursos critptográficos, de modo a assegurar a confidencialidade, a autenticidade, a integridade e o não-repúdio, assim como a interoperabilidade entre os Sistemas de Segurança da Informação;

IX - estabelecer as normas gerais para o uso e a comercialização dos recursos criptográficos pelos órgãos e pelas entidades da Administração Pública Federal, dando-se preferência, em princípio, no emprego de tais recursos, a produtos de origem nacional;

X - estabelecer normas, padrões e demais aspectos necessários para assegurar a confidencialidade dos dados e das informações, em vista da possibilidade de detecção de emanações eletromagnéticas, inclusive as provenientes de recursos computacionais;

XI - estabelecer as normas inerentes à implantação dos instrumentos e mecanismos necessários à emissão de certificados de conformidade no tocante aos produtos que incorporem recursos criptográficos;

XII - desenvolver sistema de classificação de dados e informações, com vistas à garantia dos níveis de segurança desejados, assim como à normatização do acesso às informações;

XIII - estabelecer as normas relativas à implementação dos Sistemas de Segurança da Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados, assim como assegurar a permanente disponibilização dos dados e das informações de interesse para a defesa nacional; e

XIV - conceber, especificar e coordenar a implementação da infra-estrutura de chaves públicas a serem utilizadas pelos órgãos e pelas entidades da Administração Pública Federal.

Art. 5º À Agência Brasileira de Inteligência - ABIN, por intermédio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC, competirá:

I - apoiar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante a atividades de caráter científico e tecnológico relacionadas à segurança da informação; e

II - integrar comitês, câmaras técnicas, permanentes ou não, assim como equipes e grupos de estudo relacionados ao desenvolvimento das suas atribuições de assessoramento.

Art. 6º Fica instituído o Comitê Gestor da Segurança da Informação, com atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos neste Decreto.

Art. 7º O Comitê será integrado por um representante de cada Ministério e órgãos a seguir indicados:

I - Ministério da Justiça;

II - Ministério da Defesa;

III - Ministério das Relações Exteriores;

IV - Ministério da Fazenda;

V - Ministério da Previdência e Assistência Social;

VI - Ministério da Saúde;

VII - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VIII - Ministério do Planejamento, Orçamento e Gestão;

IX - Ministério das Comunicações;

X - Ministério da Ciência e Tecnologia;

XI - Casa Civil da Presidência da República; e

XII - Gabinete de Segurança Institucional da Presidência da República, que o coordenará.

"XIII - Secretaria de Comunicação de Governo e Gestão Estratégica da Presidência da República." (NR)

§ 1º Os membros do Comitê Gestor serão designados pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, mediante indicação dos titulares dos Ministérios e órgãos representados.

§ 2º Os membros do Comitê Gestor não poderão participar de processos similares de iniciativa do setor privado, exceto nos casos por ele julgados imprescindíveis para atender aos interesses da defesa nacional e após aprovação pelo Gabinete de Segurança Institucional da Presidência da República.

§ 3º A participação no Comitê não enseja remuneração de qualquer espécie, sendo considerada serviço público relevante.

§ 4º A organização e o funcionamento do Comitê serão dispostos em regimento interno por ele aprovado.

§ 5º Caso necessário, o Comitê Gestor poderá propor a alteração de sua composição.

"XIV - Ministério de Minas e Energia;

XV - Controladoria-Geral da União; e

XVI - Advocacia-Geral da União."

Art. 8º Este Decreto entra em vigor na data de sua publicação.

Brasília, 13 de junho de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Geraldo Magela da Cruz Quintão
Luiz Felipe Lampreia
Pedro Malan
Waldeck Ornélas
José Serra
Alcides Lopes Tápias
Martus Tavares
Pimenta da Veiga
Ronaldo Mota Sardenberg
Pedro Parente
Alberto Mendes Cardoso

Publicado no DOU de 14/06/2000