

**FUNDAÇÃO GETÚLIO VARGAS**  
**ESCOLA BRASILEIRA DE ADMINISTRAÇÃO PÚBLICA E DE EMPRESAS**  
**CURSO DE MESTRADO EM GESTÃO INTERNACIONAL**  
**MASTER IN INTERNATIONAL MANAGEMENT**

**Dissertação de Mestrado apresentada por**

**MARCELO LEPSCH RAMIRO**

**Gestão da Segurança da Informação: Certificação Digital.**

**Professor Orientador Acadêmico**

**PAULO ROBERTO DE MENDONÇA MOTTA**

**Rio de Janeiro – RJ – Brasil – 2008.**

Marcelo Lepsch Ramiro

## **Gestão da Segurança da Informação: Certificação Digital.**

Dissertação de conclusão do Mestrado de  
Gestão Internacional – Master in International  
Management - ministrado pela Fundação  
Getúlio Vargas – Escola Brasileira de  
Administração Pública e Empresarial no Rio  
de Janeiro, Brasil

Orientador: Professor Paulo Roberto de Mendonça Motta.

Rio de Janeiro – RJ – Brasil – 2008.

FOLHA DE APROVAÇÃO

Marcelo Lepsch Ramiro

**Gestão da Segurança da Informação: Certificação Digital.**

Membros da Banca:

Orientador: Professor Paulo Motta.

Professores convidados: Joaquim Rubens Fontes Filho e Joel de Lima Pereira Castro Junior

Rio de Janeiro – RJ – Brasil – 2008

## Dedicatória

A minha família que me incentivou e apoiou em todos os momentos dessa caminhada.

## Agradecimentos

Ao professor Paulo Motta, pela orientação e paciência na elaboração desta dissertação.

## Epígrafe

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, atualmente art 219 da Lei nº 10.406 de 10 de janeiro de 2002 - Código Civil em vigor- (parágrafo 1º do artigo 10 da Medida Provisória 2.200-02/2001).

## **Resumo**

Cada vez mais, a informação se torna o principal ativo das instituições. Sendo assim, a Segurança da Informação (SI) vem se destacando como uma atividade de extrema importância nas corporações. Passa a ser algo primordial no cotidiano dos negócios a garantia da confidencialidade, da integridade, da disponibilidade, do não-repúdio e da legalidade. A análise do risco, passando pela avaliação das ameaças e vulnerabilidades, tem sido imprescindível para permitir o crescimento das atividades institucionais. O Certificado Digital aparece no contexto da SI para garantir a irretratabilidade, identificando de forma inequívoca o indivíduo que pratica a ação. Por isso, segurança da informação é a área do conhecimento dedicada à proteção de ativos da informação contra: acessos não autorizados, alterações indevidas, indisponibilidade, repúdio e ilegalidade.

## **Abstract**

More over, the information has become the main asset of the institutions. Being thus, the Information Security (IS) is getting attention as one of the activities of extreme importance in the corporations. Guarantee the confidentiality, integrity, availability, no deny and legality becomes something very important for the day-by-day of the businesses. An analysis of the risk, passing through the assessment of the threats and vulnerabilities, is mandatory to let grow the activities of the institutions. Digital Certification came into IS to guarantee the Not Deny (ND) because it makes the unquestioned identification of the person that makes the action. Therefore, Information Security can be defined as a knowledge field focused in the protection of the information assets against: unauthorized access, improper modifications, not availability, deny of authorship and illegality.

## Sumário

Dedicatória .....	IV
Agradecimentos .....	V
Epígrafe .....	VI
Resumo .....	VII
Abstract.....	VIII
Sumário.....	IX
Lista de ilustrações .....	XI
Lista de abreviaturas e siglas .....	XII
1. Introdução.....	1
1.1. O problema .....	2
1.2. Justificativa do estudo .....	4
1.3. Objetivos.....	4
1.3.1. Objetivo geral .....	4
1.3.2. Objetivos específicos.....	4
1.3.3. Delimitação do objeto.....	4
2. Fundamentação teórica.....	5
2.1. Informação – fator de produção.....	5
2.2. Segurança da informação.....	5
2.3. Analisando o risco .....	9
2.4. Política de segurança da informação - PSI .....	10
2.5. Classificação.....	12
2.6. Recursos humanos .....	13
2.7. Segurança física.....	15
2.8. Segurança de equipamentos móveis .....	16
2.9. Descarte de equipamentos e de documentos .....	17
2.10. Controle de acessos e auditoria de sistemas .....	18
2.11. Gestão de incidentes .....	19
2.12. Plano de continuidade de negócios - PCN.....	19
2.13. Assinatura digital .....	20
2.14. Certificação digital - CD.....	21
2.15. ISO/IEC 27001:2005 .....	23
2.16. Presente e futuro digital.....	25
3. Metodologia.....	27
3.1. Pesquisa exploratória.....	27
3.2. Estudo de caso .....	27
3.3. Seleção do Caso Único .....	29
4. Estudo de caso .....	30
4.1. A Secretaria da Receita Federal do Brasil (RFB).....	31
4.1.1. Estrutura organizacional .....	32
4.2. A Gestão da Segurança da Informação na RFB .....	35
4.2.1. A Informação – fator de produção na RFB .....	35
4.2.2. Segurança da Informação na RFB .....	35
4.2.3. Analisando o risco na RFB.....	37
4.2.4. Política de Segurança da Informação na RFB .....	38

4.2.5.	Classificação da Informação na RFB .....	39
4.2.6.	Recursos Humanos na RFB .....	41
4.2.7.	A Segurança Física na RFB.....	42
4.2.8.	Segurança de Equipamentos Móveis na RFB.....	42
4.2.9.	Descarte de equipamentos e de documentos na RFB .....	43
4.2.10.	Controle de acesso na RFB.....	44
4.2.11.	Certificação digital na RFB .....	45
5.	Discussão dos resultados .....	46
6.	Conclusão .....	48
7.	Limitações .....	49
8.	Sugestões para novas ações .....	50
9.	Bibliografia.....	LII
	Glossário.....	LVI
	Apêndice A – Questionário utilizado .....	LVIII
	Apêndice B – Política de segurança da adm. federal .....	LXII
	Apêndice C – Certificação digital na adm. federal.....	LXVIII
	Apêndice D – Criptografia .....	LXIX

## **Lista de ilustrações**

Principais ameaças à segurança da informação.....	8
Empresas no Brasil certificadas na BS 7799-2:2002 ou ISO/IEC 27001:2005 .....	23
Regiões Fiscais .....	33
Organograma da Receita Federal do Brasil.....	34
Estrutura da AC-SRF abaixo da AC-Raiz .....	46

## **Lista de abreviaturas e siglas**

CD = Certificado Digital

CID = Confidencialidade, Integridade e Disponibilidade da informação.

DoS = do inglês Deny of Service

NF-e = Nota Fiscal Eletrônica.

NR = Não Repúdio.

PCN = Plano de Continuidade de Negócios.

PSI = Política de Segurança da Informação.

RFB = Secretaria da Receita Federal do Brasil.

SPED = Sistema Público de Escrituração Digital.

UA = Unidade Administrativa.

UAs = Unidades Administrativas.

VPN = do inglês Virtual Private Network – Rede Privada Virtual.

.

# 1. Introdução

A informação tem se mostrado no século XXI como o principal ativo de uma instituição. Um grande exemplo disto pode ser visto com a empresa que tem se destacada mundialmente em curto prazo, tendo hoje, em apenas 10 anos de existência, um valor de mercado superior a maior montadora de automóveis americana. A Google tem como seu principal produto simplesmente a informação. Ela a disponibiliza gratuitamente para quem a procura e vende anúncios e espaço nas janelas mostradas para aqueles que a buscam no sítio (*site*) da empresa.

Com o avanço da informática nas últimas décadas e a queda dos preços dos computadores, mais e mais instituições estão substituindo seus arquivos de papel pelos digitais. Além disso, com a diminuição dos preços das telecomunicações, as empresas passaram a estar 24h conectadas a grande rede de computadores - a Internet – utilizando inclusive técnicas de criptografia para simular uma rede privada dentro da rede pública, conhecida como VPN (do inglês Virtual Private Network – Rede Privada Virtual). Principalmente após 2001, com o atentado às Torres Gêmeas em Manhattan, New York, Estados Unidos, todos perceberam a importância de se proteger contra ataques, anteriormente considerados pouco prováveis. O aumento dos crimes digitais e de dispositivos computacionais portáteis confirma a necessidade de se adotar padrões de segurança internacionalmente aprovados. Em 2005, foi publicada a norma ISO/IEC 27001:2005 que é uma evolução da norma BS 7799 Part 2:2002. Ela tem como objetivo a padronização de procedimentos relativos à segurança da informação, principalmente com relação aos quesitos de confidencialidade, integridade e disponibilidade (CID). Recentemente, foram incorporados os conceitos de irretratabilidade (ou não-repúdio) e de legalidade. Como grande parte das transações atualmente são digitais, é necessário proibir a utilização dos meios computacionais de forma ilegal e identificar sem margem de erro o autor das ações.

## 1.1. O problema

Um barulho é sentido avisando que já é hora de levantar para mais um dia na vida do cidadão contemporâneo. Provavelmente o sinal sonoro foi emitido não mais pelo ruído do martelinho de ferro batendo no sininho dos velhos relógios analógicos, nem tão pouco pelo badalar dos sinos da antiga igreja matriz, mas de um aparelho celular que além das funções de telefonia móvel tem diversas outras funcionalidades, incluindo aí a de despertador. Se o aparelho for um *smartphone* – telefone inteligente – estará bloqueado para utilização e solicitará uma senha para liberar o acesso ao seu conteúdo. Aqueles que são mais conscientes do perigo que é sair de casa com todas as informações pessoais e profissionais que podem ser armazenadas nestes aparelhos terão certamente um *software* – programa de computador - que implementa uma criptografia de 128bits (ou superior) para que os dados mais sensíveis só possam ser acessados após ser informada uma senha considerada forte, contendo: maiúsculas, minúsculas, números e caracteres especiais; sendo ainda superior a oito dígitos. Enquanto aguarda o café ser coado na cafeteira elétrica, ele consulta sua agenda no telefone inteligente ou *personal device assistant* - PDA – dispositivo de assistência pessoal - para o dia que se inicia e verifica que está no início do mês e há algumas contas a serem pagas além dos compromissos profissionais e sociais marcados para o decorrer do dia. Ligando a TV para escutar as notícias do telejornal matinal, ele aproveita para verificar se os canais de uso restrito estão bloqueados e solicitando senha de desbloqueio. Na garagem abrindo o seu novo carro, ele digita a senha na fechadura não precisando de chaves para entrar e dar partida no veículo. Chegando no estacionamento da empresa, ele passa o cartão de estacionamento na cancela para poder estacionar o automóvel na sua vaga tradicional. Para entrar no prédio e passar pelas catracas, ele passa o cartão de identificação com o código de barras na leitora da roleta. Chegando ao escritório, a sua assistente o informa da necessidade da sua assinatura autorizando uma movimentação de pessoal e o relembra dos compromissos do dia, pois ela tem acesso compartilhado a sua agenda profissional que é sincronizada com o telefone inteligente. Ao ligar o computador o sistema operacional solicita o usuário e a senha. Como de costume, o primeiro *software* aberto é Lótus Notes que também solicita a senha

do usuário. Após ler os e-mails e enviar alguns, ele acessa o sistema corporativo que o solicita o usuário e senha. Às 14:00h, indo para o restaurante almoçar, ele lembra de passar no banco para pagar algumas contas e retirar um pouco de dinheiro. O terminal eletrônico solicita o cartão do banco e a senha numérica. Para confirmar a operação, é solicitada uma nova senha alfanumérica. Já no restaurante, ele lembra de acessar seu correio eletrônico na Internet através da conexão WiFi que o solicita uma senha de conexão do Hotspot – lugar de acesso à Internet via rede WiFi. O Gmail, seu provedor do correio eletrônico na Internet, solicita o usuário e senha para liberar o acesso à caixa postal. No final do almoço, ele usa o cartão de crédito com chip e o garçom traz a “maquininha” na mesa para que seja digitada a senha. Retornando ao trabalho, ele faz acesso a alguns outros sistemas satélites ao sistema corporativo, cada um solicitando um usuário e senha específicos. Ao sair do trabalho, ele deixa o carro no estacionamento e pega o metrô para ir a uma consulta médica. Para passar pela roleta do Metrô, ele passa o cartão eletrônico onde há créditos para a utilização deste transporte coletivo. Enquanto aguarda a composição, ele usa o celular para pagar o refrigerante da máquina na plataforma. Chegando ao consultório, a secretária solicita o cartão do convênio e a senha do usuário para efetuar o pagamento da consulta. Já retornando para casa no seu veículo, ele passa na locadora para alugar um HD DVD tendo que mostrar o cartão de associado ao atendente e digitar a senha correspondente. Já em casa, ele lembra que tem que fazer uma ligação pelo Skype ao seu amigo europeu e faz a conexão de alta velocidade do provedor Velox digitando a senha e depois acessa o software de comunicação informando o usuário e senha. Após toda a confusão do dia, ele resolve antes de dormir assistir um filme no canal bloqueado por senha da TV por assinatura.

O texto acima mostra a confusão atual em que se encontra o cidadão moderno no seu dia-a-dia. São vários cadastros, cartões e senhas para se memorizar. Sem falar nos sistemas que obrigam o usuário a mudar a senha de tempos em tempos, não permitindo que as senhas anteriores sejam reutilizadas. Há ainda o problema que alguns cadastros exigem senhas alfanuméricas e outros que só permitem números. Fica impossível a memorização todas as senhas e contas de acesso sem se anotar tais informações em algum lugar, tornando estes sistemas vulneráveis. Por isso, há a necessidade da criação de um mecanismo de identificação eletrônica único e confiável para que possa ser usado em todos os cadastros e sistemas de identificação do cidadão, tal como são solicitados hoje o número do CPF e a

carteira de identidade deste. Tal cartão já existe e é conhecido como Smart Card, mas sua utilização depende de algo mais: a conscientização do usuário.

## **1.2. Justificativa do estudo**

A falta de uma padronização leva o usuário a escrever suas identificações nos sistemas (usuários e senhas) em papéis para evitar o esquecimento e o seu bloqueio nos programas de computador necessários ao desempenho de suas atividades profissionais e pessoais. Isto faz com que todos os procedimentos e tecnologias aplicados na segurança dos sistemas fiquem expostos a uma simples observação destas senhas por aqueles que têm a intenção de acessá-los indevidamente. Outra situação é a identificação precisa do autor da ação, pois havendo compartilhamento das contas e senhas não se pode precisar quem realizou a operação. Por isso, faz-se necessário um mecanismo que substitua todas as contas e senha por um único meio de identificação confiável e que seja de fácil utilização.

## **1.3. Objetivos**

### **1.3.1. Objetivo geral**

Identificar qual a tecnologia que pode resolver o problema das diversas contas de usuário e múltiplas senhas para se memorizar, não afetando a confidencialidade, integridade e disponibilidade dos sistemas, garantindo a irretratabilidade dentro da legalidade.

### **1.3.2. Objetivos específicos**

Verificar a praticidade do certificado digital e a sua segurança.

### **1.3.3. Delimitação do objeto**

Este trabalho está limitado aos sistemas da Receita Federal do Brasil. Sendo assim, todas as necessidades de segurança da informação apresentadas neste trabalho são relativas ao cenário sócio-econômico brasileiro.

## **2. Fundamentação teórica**

### **2.1. Informação – fator de produção**

Afinal, o que é informação? Segundo o dicionário Houaiss, informação é o “conjunto de conhecimentos reunidos sobre determinado assunto”, mas de acordo com o dicionário Aurélio, informação é o “conjunto de dados acerca de alguém ou de algo”. Basicamente, as pessoas necessitam de informação para a tomada de decisões buscando os fins desejados (acerto), evitando o “achismo” (intuição). Fica claro que a informação é essencial, pois sem ela não existe planejamento. Sendo assim, é de extrema importância garantir a CID - confidencialidade, integridade e disponibilidade da informação. Vale lembrar que ela pode estar armazenada de diversas maneiras: na mente das pessoas, em imagens armazenadas em fotografias e filmes, impressa ou em meios magnéticos e eletrônicos (flash cards, pen drives, DVDs, discos etc). Para tratar de segurança da informação é preciso raciocinar em todos os meios utilizados para o armazenamento da informação buscando sempre a sua CID. Ela deve ser considerada como um ativo da empresa com a mesma relevância de outros bens tangíveis, uma vez que deve ser protegida contra: furtos, vandalismo, problema ambiental, danos provocados ou acidentais.

Desde a antiguidade, o ser humano percebeu a importância de se passar a informação para gerações futuras. Ele desenhou gravuras nas cavernas para mostrar o seu dia-a-dia. O primeiro registro de linguagem escrita data de aproximadamente 4.000 anos antes de Cristo na Suméria e a partir de então outras civilizações criaram suas próprias formas de registrar e transmitir a informação, tais como: hieróglifos, ábaco, papel, fotografia e finalmente em meio digital.

### **2.2. Segurança da informação**

Na história da civilização, houve sempre a preocupação para proteger a informação principalmente contra catástrofes naturais, degradação do meio de arquivamento, saques e incêndios. As bibliotecas foram as primeiras instituições a prestarem este papel. Elas

guardam e protegem a informação para consultas futuras. Com o tempo, outra preocupação que surgiu foi com relação a confidencialidade da informação. Para isso foram criados diversos mecanismos de criptografia da informação principalmente quando havia a necessidade de se transportar a informação de um ponto a outro. Fazendo com que se a informação fosse interceptada no meio do caminho, ela não pudesse ser compreendida.

Na história moderna um grande exemplo da utilização de criptografia foi a máquina desenvolvida pelos alemães denominada “Enigma” que foi utilizada para enviar e receber mensagens entre os militares alemães na Segunda Guerra Mundial sem que os aliados conseguissem entender o seu conteúdo quando capturada. Com a proliferação dos computadores e a sua ligação em redes, privadas e públicas, houve a necessidade de se criar meios que impedissem o acesso e a modificação indevidos das informações.

O resultado disto foram as diversas publicações de normas de segurança surgidas pelo mundo. Considerada a primeira norma que apresentou soluções para o tratamento da informação de forma mais abrangente, a BS-7799 foi publicada pelo Comercial Computer Security Centre e é a base da atual ISO/IEC 27001:2005 que entrou em vigor em novembro de 2005.

O governo brasileiro publicou o Decreto Presidencial nº 3.505 em 13 de junho de 2.000 (ver apêndice B na página LXII) regulamentando a segurança da informação nos órgãos e nas entidades da administração pública federal. Salienta-se o artigo 3º inciso I que consta:

“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.”

A expansão dos sistemas computacionais facilitou o compartilhamento de recursos e informações. Porém, não só benefícios vieram com essa grande conectividade, tal como a Internet, mas também diversas ameaças. A segurança da informação não pode mais se preocupar apenas com a perda de dados relacionada a um acidente com os meios de arquivamento. Há agora a ameaça de ataques via rede, vandalismos ou técnicas de negação de serviço – DoS – do inglês Deny of Service. Além disso, existe ainda o perigo do ataque

interno, cometido por colaboradores das instituições com acesso aos recursos físicos e lógicos.

Na implantação de mecanismos de segurança da informação é busca-se o equilíbrio entre custo e benefício. Com raras exceções, principalmente quando a vida humana está envolvida, não se gasta mais com segurança que o valor da informação a ser protegida. O grande problema é como mensurar este valor, pois seu contexto abrange a proteção da informação em si, dos sistemas computacionais, da infra-estrutura de rede e dos serviços que a dão suporte, contra imprevistos, assaltos e falhas na manipulação.

A informação é um bem tal como vários outros, portanto deve ser vista como um “Ativo” da instituição. Ela deve ser mantida pelo tempo necessário conforme seu grau de importância. As interligações das empresas através das redes de computadores, pessoas e eventos naturais, podem mostrar as vulnerabilidades que põem em risco as informações. Por isso, é necessária a implantação de processos de segurança que resguardem a informação contra essas ameaças.

Entende-se:

- Ameaça como uma possível causa de um acidente indesejado, que caso se materialize pode ocasionar prejuízo à instituição;
- Ativo é tudo aquilo que tem valor para uma instituição ou pessoa, tais como: computadores, softwares, capacidade de fabricar algum produto ou serviço, imagem, marca, patente etc...
- Vulnerabilidade é a fraqueza ou restrição de um ativo que pode ser atacada por uma ou mais ameaças.
- Risco é a combinação de possibilidade da consolidação de uma ameaça e os resultados do impacto causado por este episódio.

Peixoto (2006) classifica ainda as ameaças como sendo:

- Naturais – decorrem de fenômenos da natureza, tais como: terremotos, enchentes, queda de raios etc;
- Involuntárias - ocorrem devido a acidentes;
- Voluntárias - quando propositas, de ocorrência humana.

Já as vulnerabilidades podem ser:

- Físicas - tais como estrutura de segurança fora dos padrões exigidos;
- Naturais - pois os computadores são propensos a sofrerem com variações da natureza tais como umidade e temperatura;
- Hardware - onde todos os equipamentos são sujeitos a falhas, tais com fadiga do material;
- Software - quando mal instalado, por exemplo;
- Mídias - pois elas são suscetíveis a falhas devido a diversos motivos, dentre eles a radiação eletromagnética;
- Comunicação - devido a acessos não autorizados ou perda de comunicação;
- Humanas - tais como o não seguimento das políticas de segurança.

Menezes (2006) apresenta em seu trabalho uma tabela (Quadro 1) produzido pela Modulo Security Solutions S.A na 9ª Pesquisa Nacional de Segurança da Informação realizada em outubro de 2003 chamando a atenção para “Funcionários insatisfeitos” e “Vazamento de informações”, assim como “Divulgação de senhas” e “Acessos indevidos” como os principais itens contra os quais são necessárias medidas preventivas.

Principais ameaças à segurança da informação.

<i>Vírus</i>	<i>66%</i>
<i>Funcionários insatisfeitos</i>	<i>53%</i>
<i>Divulgação de senhas</i>	<i>51%</i>
<i>Acessos indevidos</i>	<i>49%</i>
<i>Vazamento de informações</i>	<i>47%</i>
<i>Fraudes, erros e acidentes</i>	<i>41%</i>
<i>Hackers</i>	<i>39%</i>
<i>Falhas na segurança física</i>	<i>37%</i>
<i>Uso de notebooks</i>	<i>31%</i>
<i>Fraudes em e-mail</i>	<i>29%</i>

Obs.: o total de citações é superior a 100% devido à questão aceitar múltiplas respostas.

É através da implantação de diretrizes, normas, procedimentos e controles adequados que se obtém a segurança da informação, garantindo a operação da instituição, enfrentando as ameaças que ela está propensa e preservando os três princípios básicos (CID): Confidencialidade, Integridade e Disponibilidade, mais o não-repúdio e a legalidade, onde:

- Confidencialidade é a garantia de que somente pessoas autorizadas previamente possam ter acesso a informação;
- Integridade é a garantia de que a informação só possa ser alterada por pessoa autorizada;
- Disponibilidade é a garantia de que a informação estará sempre disponível quando for necessário o seu acesso;
- Não-repúdio ou irretratabilidade é a garantia que o autor da ação não poderá negar a sua autoria; e
- Legalidade é a garantia que todas as operações serão dentro dos procedimentos, normas, diretrizes e legislação vigente.

### **2.3.      *Analizando o risco***

Uma boa definição de risco, para a área de segurança da informação, foi dada por *Sêmola* (2003): “risco é a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e/ou disponibilidade, causando, possivelmente, impactos nos negócios”. Analisar risco é avaliar ameaças e vulnerabilidades. O primeiro passo na confecção e gestão de um programa de segurança é a identificação de ameaças e riscos mais significantes, pois isto permitirá determinar os trabalhos necessários para minimizá-los. Em seguida, os riscos precisam ser qualificados para que sejam classificados de acordo com a aceitação dos riscos e dos objetivos da instituição. Estas são apenas algumas das atividades de tantas outras de gerenciamento de riscos, tais como: implementar políticas apropriadas e controles relacionados, promover a conscientização das medidas adotadas, monitorar e avaliar as políticas e seus controles efetivos. Riscos e ameaças mudam com o tempo, é necessário que a instituição faça uma reavaliação periódica destes, revendo as políticas e controles adotados.

De forma geral, as etapas para se avaliar os riscos de uma operação são:

- conhecer as ameaças com potencial para causar prejuízos, tais como: invasões, roubos, colaboradores desleais, ataques externos e eventos da natureza;

- verificar a probabilidade da ocorrência destas ameaças segundo o histórico dos eventos e sensibilidade das pessoas envolvidas no processo;
- quantificar o valor do prejuízo caso a ameaça venha a se concretizar, determinando assim os ativos mais significativos;
- verificar a despesa necessária para reduzir ou eliminar o risco;
- registrar os resultados dos levantamentos anteriores e fazer os planos de ação.

Vale notar que não existe operação sem risco (*risk free*). A análise de riscos é fundamental para se identificar os riscos e ameaças que os sistemas de tecnologia da informação e comunicação e os seus ativos estão sujeitos, com o objetivo de identificar e escolher as contramedidas necessárias. Os riscos são classificados como sendo: alto, onde contra-medidas são executadas imediatamente para se evitá-lo; médio, requerendo a implantação de contramedidas em médio prazo; baixo, onde as contramedidas podem ser aplicadas em longo prazo ou nem mesmo implantadas. Já as ameaças podem ser qualificadas como: alta, onde há um histórico de ocorrências expressivo e pode ocorrer a qualquer momento; média, onde existe algum histórico e por isso uma probabilidade razoável de ocorrer novamente; baixa, não havendo histórico e quase improvável que venha ocorrer; não aplicável, significando que a ameaça não é crítica para a situação analisada. .

Alves (2006) afirma que: “...o tratamento contínuo do risco é de fundamental importância para que as empresas obtenham informações mais precisas quanto aos pontos fracos dos seus sistemas, pessoas, ambiente etc. e possam tratá-los de acordo com os melhores critérios definidos de acordo com o perfil da organização.”

## **2.4. Política de segurança da informação - PSI**

Lemos (2001) sintetiza a PSI como: “São normas que definem as melhores práticas para o manuseio, armazenamento, transporte e descarte das informações, sendo uma ferramenta para a prevenção e proteção da informação, de forma a restringir acessos e salva-guardar a sua manipulação por pessoas não autorizadas”.

Segundo Sêmola (2003) a PSI: “estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa”.

Ramos (2006) escreveu que: “a Política de Segurança da Informação de uma organização é um conjunto de documentos que descreve quais são os objetivos que todas as atividades ligadas a Segurança da Informação (SI) devem trabalhar para atingir...Ela resume os princípios de SI que a organização reconhece como sendo relevantes e que devem estar presentes no dia-a-dia de suas atividades.”

A PSI não é algo trivial a ser desenvolvido, mas como a literatura diz: “...é preferível uma política mal escrita do que nenhuma política...”. Há algumas etapas a serem seguidas para a confecção de uma política:

- Escrever um esboço da política, procurando fazer um documento com foco nos processos de negócio e não na tecnologia, mostrando quais as operações estão em risco;
- Apresentar o esboço à diretoria objetivando conseguir o engajamento da direção sendo este apoio fundamental para o seu sucesso;
- Criar um comitê de PSI formado por pessoas de setores distintos da instituição interessadas na implantação de uma boa política de segurança. O comitê terá a função de escrever as diretrizes e normas da PSI;
- Divulgar a política para todos da organização e aqueles que interagem com ela, os chamados *stakeholders*, sendo interessante que as pessoas tenham conhecimento daquilo que precisam saber para se ter um ambiente seguro (informação certa para a pessoa certa);
- Levar a política a sério tal como se faz com as leis, pois uma boa política deve prever advertências e punições para quem não a cumprir, assim como premiação para quem a cumprir com afinco;
- Aceitar sugestões é sempre uma boa prática, pois as pessoas que trabalham com os procedimentos são as mais indicadas para avaliá-los no dia-a-dia;
- Reavaliar periodicamente a política e suas emendas, pois as instituições são dinâmicas e todos os procedimentos devem ser revistos pelo menos uma vez ao ano;
- Refazer todo o processo após a reavaliação realizada na etapa anterior.

Segurança é uma questão que está relacionada principalmente a pessoas, mais do que aspectos físicos ou tecnológicos. Sendo assim, é primordial que existam procedimentos que se preocupem com atenção das pessoas que acessam as informações da instituição. A quebra do sigilo das informações por empregados ou terceirizados é um dos maiores riscos para a segurança da informação, podendo ocorrer intencionalmente ou não. É aconselhável que sejam feitos acordos de confidencialidade das informações acessadas tanto por pessoas internas da organização como pelas externas. Estes acordos precisam estar conforme a legislação aplicável permitindo que no caso de violação destes acordos o Judiciário venha a ser acionada.

## **2.5. Classificação**

Ao longo do tempo a informação tem a característica de perder o seu valor, tornando-se pública e até não interessando a mais ninguém. É essencial que ela seja classificada e esta classificação seja revisada de tempos em tempos. Esta classificação deverá considerar o prejuízo que sofrerá a instituição em caso de quebra de confidencialidade, integridade e disponibilidade da informação. Para que este objetivo seja alcançado são necessárias definições de categorias com relação à criticidade da informação. Esta classificação será feita pelo gestor de cada informação e reclassificada de acordo com os requisitos de confidencialidade que mantém perante a instituição. Um bom exemplo deste fato é um evento de premiação que tem classificada como secreta a informação antes do anúncio dos vencedores e sem classificação (pública) logo após a divulgação destes. Um princípio que deve ser sempre seguido quando do acesso a informação é o do “mínimo privilégio”, onde cada usuário somente terá acesso ao que realmente precisa para a realização das suas tarefas. No Brasil, há o Decreto Federal nº 4.553/2002 para a administração pública com as seguintes classificações:

- Ultra-secretos: informações cujo conhecimento possa acarretar em dano excepcionalmente grave à segurança nacional;
- Secretos: informações cujo conhecimento possa acarretar em dano grave à segurança nacional;

- Confidenciais: informações cuja revelação pode frustrar seus objetivos ou causar dano à segurança da sociedade e ao estado;
- Reservados: informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos;

No âmbito comercial as informações são classificadas da seguinte forma:

- Confidencial: se a informação for revelada a empresa poderá ser afetada seriamente;
- Privada: informação sobre o corpo funcional;
- Sensível: requer precauções especiais;
- Proprietária: poderá reduzir a competitividade da empresa se for revelada;
- Pública: se revelada não afetará a instituição.

Ressalta-se que a informação classificada deve sofrer controles que garantam o seu sigilo quando do armazenamento, transporte e manuseio, permitindo assim um rastreamento em caso de quebra de segredo.

## **2.6.     *Recursos humanos***

A S.I. precisa levar em conta a segurança em recursos humanos, constituídos por funcionários, prestadores de serviço, executivos e acionistas, em três momentos: antes da contratação, durante a execução das atividades e no encerramento do contrato. Toda função profissional precisa ter suas responsabilidades claramente definidas e de conhecimento das pessoas que irão exercê-las. Antes da contratação o candidato deve concordar com a função que irá exercer na instituição, sendo suas responsabilidades definidas em documento que descreve as condições da contratação. Salienta-se que todo candidato a exercer uma função na empresa deve ser avaliado com relação à sua capacidade de exercê-la, levando em conta as características pessoais, alinhamento às regras, exercício da responsabilidade, experiência profissional, tratamento adequado de informações de diferentes níveis de confidencialidade e concordância com a política de segurança da instituição. A descrição de função deve conter a obrigatoriedade de se seguir a política de

segurança, proteger os ativos, executar as orientações e avisar aos superiores qualquer situação de risco.

A seleção de pessoal é uma fase muito fundamental. Nela evita-se ao máximo a contratação de pessoas de índole duvidosa, checando se as informações prestadas são verdadeiras e se a situação de crédito e registros criminais estão normais. Os termos e condições de contratação de colaboradores, fornecedores e outros profissionais devem contemplar a política de segurança da organização, incluindo: responsabilidade pelo tratamento da informação recebida, responsabilidades legais e direitos, responsabilidades fora da organização, assinatura do termo de confidencialidade, sanções em caso de desrespeito aos requisitos de segurança e responsabilidade pela classificação da informação. Para o sucesso da segurança da informação é imprescindível que todos aqueles que trabalhem para a organização apoiem a política de segurança e demais regulamentos, saibam quais são as suas responsabilidades e estejam conscientes dos controles necessários para a manutenção do nível adequado de segurança. O engajamento da direção da empresa no processo de SI é indispensável para o êxito da PSI, assegurando que todos estejam instruídos de suas responsabilidades. Para isso, as pessoas devem ser constantemente: instruídas sobre suas responsabilidades e uso correto quando do acesso à informação, motivadas a cumprir todos os regulamentos de SI, conscientizadas em relação à PSI e capacitadas para atender os requisitos de segurança exigidos. Sanções e processo disciplinar precisam ser estabelecidos para aqueles que não cumprirem os regulamentos.

Uma medida a ser tomada, principalmente para se evitar fraudes, é o princípio de segregação. Funções potencialmente conflitantes, como autorização, aprovação, execução, controle e contabilização das operações devem ser executadas por pessoas diferentes permitindo a conferência dos trabalhos evitando-se assim incorreções.

Quando do encerramento das atividades junto à empresa por parte dos funcionários, fornecedores e terceiros, deve haver um procedimento que realize de forma ordenada e controlada esta rescisão, retirando o acesso destes aos recursos de informação e lembrando-os do contrato de sigilo assinado no ato da contratação, quando for o caso.

## **2.7.     *Segurança física***

A segurança física tem como objetivo fornecer um ambiente seguro para todos os ativos da instituição, inclusive as atividades envolvendo sistemas de informação. A segurança física pode ser alcançada utilizando-se guardas, trancas, alarmes, circuito fechado de TV etc. Ela é muito importante porque se for ultrapassada, vários controles de segurança lógicos poderão ser contornados, liberando acesso aos ativos. Por exemplo, uma pessoa com acesso a um computador pode reiniciá-lo com outro sistema operacional e ter acesso às informações contidas no mesmo. A integridade dos dados é facilmente quebrada após se romper a barreira física.

Algo importante a ser notado é que como os sistemas estão interligados, a segurança final estará relacionada a segurança do elo mais fraco. Por isso, não adianta ter uma sala cofre, repleta de mecanismos de segurança se houver algum servidor sem proteção ligado aos servidores da sala cofre.

Outra consideração importante é quanto ao local de guarda das mídias de cópia de segurança, pois elas possuem informações do negócio da instituição e caso sejam interceptadas haverá a quebra da confidencialidade. Elas devem ser armazenadas em local fisicamente distante dos dados originais, pois em caso de acidentes tais como incêndio, elas não sejam atingidas.

O controle de entrada física também merece bastante atenção. Todas as pessoas que circulam pelas instalações devem portar crachás de identificação, de preferência com fotografia atualizada. Os visitantes nunca devem permanecer desacompanhados de um responsável. Locais com informações sensíveis devem possuir controles adicionais, tais como controles biométricos. É recomendada a verificação periódica dos acessos concedidos, revogando aqueles que não são mais necessários. Um conceito interessante a ser utilizado é o de necessidade de conhecimento (Need to Know). Ambientes considerados seguros não devem ser identificados para dificultar sua localização por quem não é autorizado a ter acesso. Somente aqueles que necessitem acessá-los devem conhecer a sua localização dentro da organização e quais os métodos de acesso e mecanismos de proteção dos mesmos.

Importante também é assegurar a saúde e segurança das pessoas que trabalhem nas instalações da instituição, pois os colaboradores da instituição são valiosos ativos de informação. Além de garantir um ambiente agradável, a empresa não pode implementar um sistema de proteção que ameace a integridade de seus trabalhadores.

As instalações hidráulicas e elétricas devem ser revisadas periodicamente para evitar que materiais de fácil combustão fiquem próximos a áreas protegidas. É importante que os equipamentos de combate a incêndio estejam em locais de fácil acesso e sejam revisados periodicamente.

É necessário evitar que pessoas externas à organização tenham acesso a áreas de carga e descarga sem permissão. De preferência, estes locais devem ficar distantes das áreas seguras da instituição. Em especial, os materiais entregues precisam ser verificados antes de serem aceitos.

Os dados que estejam sendo manipulados não podem ser facilmente observados por pessoas que não tenham autorização para ter acesso a estas informações.

O consumo de alimentos e fumo próximo aos equipamentos precisa ser proibido para se evitar acidentes causando danos e perdas dos equipamentos e por consequência da informação.

Especial atenção deve ser dada aos cabos de comunicação, pois eles podem ser usados para interceptação não autorizada dos dados. Por isso, periodicamente inspeciona-se as passagens e canaletas a procura de equipamentos de espionagem.

Não há operação 100% livre de risco. Como exemplos de eventos que fogem ao controle da instituição e que são de difícil prevenção pode-se citar: efeitos da natureza (terremoto), fornecedores de suprimentos (queda de torre de transmissão de energia), queda de aeronaves e ataques terroristas. Por isso, sempre que possível é importante haver um Plano de Continuidade de Negócio (PCN – ver página 19) quando eventos semelhantes aos anteriores vierem a ocorrer.

## **2.8.     *Segurança de equipamentos móveis***

Com o advento da computação móvel fez-se necessária a utilização de alguns novos procedimentos visando a segurança dos ativos que circulam fora do ambiente institucional. Principalmente em locais onde haja maior risco de extravio destes aparelhos, como por

exemplo, nos aeroportos, onde quadrilhas especializadas atuam no roubo de computadores portáteis. Atualmente, as pessoas que ocupam posições hierárquicas superiores nas instituições possuem notebooks e os levam com frequência para fora da empresa em viagens, reuniões, residência etc. Estes colaboradores são justamente aqueles que trabalham com informações sensíveis ao funcionamento da empresa. Há grande importância em se implantar mecanismos de segurança nestas ferramentas móveis como por exemplo a implantação de áreas de armazenamento de informações com a utilização de criptografia e o uso de protocolos seguros de comunicação para a interligação destes aparelhos com o ambiente corporativo utilizando a Certificação Digital (CD – ver página 21) além da cópia de segurança (backup) dos dados contidos nestes aparelhos. Estes procedimentos são extremamente importantes, pois com o nível de violência atual com roubos de veículos e transeuntes em números elevadíssimos, não são poucos os casos de perda de computadores, telefones inteligentes (*smartphones*), dispositivos de assistência pessoal (PDA – *Personal Device Assistant*), memórias eletrônicas (*pendrives*) e conseqüentemente das informações contidas nestes equipamentos caso não estejam criptografadas e não tenham cópia de segurança (backup).

## **2.9. Descarte de equipamentos e de documentos**

Com o advento de técnicas de recuperação de dados, mesmo em discos com mau funcionamento, fez com que o descarte de equipamentos obsoletos deva ser feito segundo os padrões de segurança da informação. Dependendo do grau de sensibilidade dos dados, os dispositivos de armazenamento devem ser destruídos.

Qualquer retirada de equipamento da organização deve ser feita de forma controlada e protegida, evitando-se que equipamentos que contenham informações sensíveis sejam retirados da empresa sem a devida autorização.

Para o descarte de documentos utiliza-se máquinas trituradoras de papel de forma que seja impossível a reconstituição do papel triturado. Poucos são os setores das instituições que utilizam estas máquinas além do Departamento de Gestão de Pessoal, quando na realidade há informações estratégicas muito mais sensíveis sendo lançadas em lixeiras comuns sem o devido cuidado com o descarte. A espionagem industrial é fato e

não mito. Diante disso, todo cuidado é necessário para que as informações sigilosas das empresas não caiam em mãos erradas.

## **2.10. Controle de acessos e auditoria de sistemas**

Tudo é proibido exceto o que é expressamente permitido! Esta é a premissa básica. Os controles de acesso têm o objetivo de proteger equipamentos, aplicações, arquivos e dados contra perda, modificação ou divulgação não autorizada. Através deste controle é possível determinar quais recursos podem ser acessados e que tipo de acesso pode ser realizado. Regras de controle de acesso devem ser criadas baseadas nas políticas de autorização e divulgação da informação, levando-se em conta os requisitos de segurança das aplicações do negócio, a identificação de todas as informações referentes às aplicações, a consistência entre controle de acesso e políticas de classificação da informação, a legislação aplicável e obrigações contratuais.

Através da auditoria, é possível determinar que tipo de acesso foi realizado a um recurso, por quem e quando. Calheiros (2004) destaca a auditoria como sendo um dos objetivos da PSI e diz que sua finalidade é “proteger os sistemas contra erros e atos cometidos por usuários autorizados identificando autores e ações, utilizando trilhas de auditorias e *logs*, que registram o que foi executado no sistema, por quem e quando”. Lemos (2001) complementa esta informação dizendo que: “a função do auditor de sistemas é zelar para que as providências planejadas estejam sendo desempenhadas conforme o previsto e planejado, analisando-se aspectos como o de atendimento aos recursos orçados, sigilo das informações a dados processados pelos sistemas de informações empresariais, manutenção do processo de produção de software em bons termos, conforme planos empresariais, cuidando para que sua função seja desempenhada no máximo sigilo, discrição, responsabilidade, compreensão dos envolvidos e atualizada nos termos técnicos que dizem respeito à produção de software”.

### **2.11. Gestão de incidentes**

Havendo uma violação na política de segurança, atua-se de forma a seguir um procedimento preciso previamente definido para tais eventos. Todos da instituição precisam conhecer um ponto de contato sempre disponível para o registro destes fatos. Apesar de se pensar em invasão quando se fala em incidente de segurança, na realidade tudo que prejudique a Confidencialidade, Integridade e Disponibilidade (CID) é considerado como incidente de segurança da informação. Como por exemplo: mau funcionamento de um sistema ou mau funcionamento de um hardware.

Ainda melhor que avisar sobre um evento de violação é a comunicação sobre uma fragilidade que possa permitir um incidente. É preciso incentivar as pessoas da instituição a ajudarem na melhoria do processo de segurança da informação.

Um princípio básico em gestão é que: “o que não se conhece não se controla, o que não se controla não se mensura, o que não se mensura não se gerencia, o que não se gerencia não se aprimora”. Por isso, o registro dos incidentes é uma valiosa fonte de informação para se verificar os eventos e a necessidade de implantação de novos controles que permitam a medição dos ocorridos, admitindo um gerenciamento dos fatos, possibilitando o aprimoramento contínuo do processo e justificando, quando for o caso, um maior investimento em algum controle específico.

### **2.12. Plano de continuidade de negócios - PCN**

Com o objetivo de se minimizar os impactos de um desastre, garantindo a continuidade das atividades principais da instituição num curto espaço de tempo minimizando os choques, desenvolve-se o Plano de Continuidade de Negócios (PCN). Ele é feito com a intenção de contingenciar situações e incidentes de segurança que não puderem ser evitados. Devido a sua complexidade, normalmente as instituições possuem diversos planos de continuidade integrados e direcionados a diferentes atividades e características da empresa. Esta segmentação é importante, pois existem vários processos com níveis diferentes de tolerância a falhas assim como os impactos. Sêmola (2003) destaca ainda três planos de contingência que são desenvolvidos para cada ameaça: plano

de administração de crise, que define os procedimentos a serem executados antes, durante e depois da ocorrência de um incidente; plano de continuidade operacional, que define os procedimentos para contingenciamento dos ativos que suportam os processos de negócio; e plano de recuperação de desastres, que define os procedimentos de recuperação e restauração das funcionalidades dos ativos afetados pelo incidente.

Maior (2006) escreve que: “O processo de continuidade deve ser implementado para reduzir a interrupção causada por um desastre ou falha na segurança para um nível aceitável através de uma combinação de ações preventivas e de recuperação. As consequências de desastres, falhas de segurança e perda de serviços devem ser analisadas. Os planos de contingência devem ser desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados no tempo devido”.

### **2.13. Assinatura digital**

Assinar documentos faz parte da rotina de qualquer pessoa. Assim como no mundo físico, o mundo digital também necessita de uma assinatura. Através da utilização da criptografia assimétrica e funções hashing a assinatura digital se tornou realidade.

O funcionamento da assinatura digital ocorre da seguinte forma: é necessário que o usuário tenha um documento eletrônico (Certificado Digital) e a chave pública do destinatário (um usuário pode ser tanto uma pessoa quanto uma instituição qualquer). Através de programas apropriados, o documento é então criptografado de acordo com a chave pública do destinatário e assinado com a chave privada do remetente. O receptor usará então sua chave privada correspondente (que é exclusiva dele) para decriptografar o arquivo e verificar a assinatura do remetente através da chave pública deste. Se qualquer bit do documento for alterado a assinatura será deformada, invalidando o arquivo.

O processo de assinatura digital de documentos eletrônicos usa um conceito conhecido como **função hashing**. Como o uso de um sistema de criptografia assimétrico nas assinaturas digitais pode causar muita demora numa decifragem, a função hashing se mostrou como a solução ideal. Seu funcionamento ocorre da seguinte forma: a função hashing analisa todo o documento e com base num complexo algoritmo matemático gera um valor de tamanho fixo para o arquivo. Esse valor, conhecido como "valor hash", é

calculado com base nos caracteres do documento. Isso deixa claro que o arquivo em si não precisa, pelo menos teoricamente, ser criptografado (caso não seja algo secreto), mas sim acompanhado do valor hash. Com isso, qualquer mudança no arquivo original, mesmo que seja de apenas um único bit, fará com que o valor hash seja diferente e o documento se torne inválido.

É interessante notar que é praticamente impossível descobrir a chave privada através da chave pública. Isso se deve ao algoritmo aplicado. Se usado o método RSA (**R**ivest, **S**hamir and **A**dleman) - dois números primos muito grandes são multiplicados. O resultado é a chave pública. Para descobrir os dois números que a geraram é necessário fazer uma fatoração, mas isso é impraticável com o poder computacional atual.

## **2.14. Certificação digital - CD**

O Certificado Digital (CD) funciona como uma carteira de identidade virtual. Lacorte (2005) diz que o CD é um documento eletrônico que contém diversos dados sobre o emissor, a Autoridade Certificadora (AC) e o titular do certificado, como: nome do titular, identificação do algoritmo de assinatura, assinatura digital do emissor, validade do certificado e dois números denominados chave pública e privada. A chave privada é que garante o sigilo dos dados do titular que assina a mensagem. A pública permite que ele compartilhe com outras pessoas a informação protegida por criptografia.

A Certificação Digital permite a assinatura eletrônica, tornando mais segura a prática de atividades online, como o uso de Internet banking, compras online e declaração de Imposto de Renda. Por exemplo, em transações bancárias, o banco terá a certeza de que quem está acessando sua conta corrente é o cliente portador do certificado digital, evitando fraudes. No entanto, ao contrário do RG, a certificação digital tem validade. O prazo de vigência do documento eletrônico varia em função do tipo de certificado.

A emissão da Certificação Digital só pode ser feita presencialmente. O interessado deve procurar uma AC, preencher um formulário com seus dados e pagar uma taxa que varia de acordo com o modelo do documento eletrônico. Depois disso, o solicitante apresenta-se em uma Autoridade de Registro (AR), com documentos como Carteira de Identidade ou Passaporte - se for estrangeiro-, número do CPF, Título de Eleitor, comprovante de residência e número do PIS/PASEP. Pessoas jurídicas devem apresentar

registro comercial, no caso de empresa individual, ato constitutivo, estatuto ou contrato social, número do CNPJ e documentos pessoais da pessoa física responsável.

A Receita Federal do Brasil registrou, no ano de 2007, a entrega de 120 mil declarações do Imposto de Renda da Pessoa Jurídica (DIPJ) transmitidas pela internet mediante certificação digital. Essa tecnologia oferece ao contribuinte a possibilidade de cumprir suas obrigações fiscais pela Internet. Em 2006, apenas 12 mil grandes empresas tinham acesso à certificação digital.

De acordo com o supervisor nacional do Imposto de Renda, Joaquim Adir, o certificado digital está facilitando a vida de milhares de contribuintes: "Com a tecnologia, o contribuinte resolve todas as pendências sem precisar ir ao balcão da Receita, por exemplo". Adir diz também que o objetivo da Receita é que parte das micro e pequenas empresas tenha acesso a essa tecnologia num futuro próximo.

O contribuinte que tiver certificação terá acesso a todos os serviços e informações protegidos por sigilo fiscal disponíveis no e-CAC, portal de atendimento virtual da RFB. Pode ainda resolver pendências cadastrais, informar e trocar dados e informações com a Receita de forma ágil e segura, além de verificar e consultar o resultado do processamento da declaração do Imposto de Renda, retificar o Documento de Arrecadação a Receita Federal, obter cópia de pagamento e negociar parcelamento. Possibilita ainda ao titular delegar a terceiros o uso do certificado através de procuração eletrônica.

Freitas (2002) destaca que com o Certificado Digital é possível a realização de 4 princípios básicos: a identificação das partes envolvidas em uma transação, garantia da integridade, o sigilo e a impossibilidade de repúdio.

Lacorte (2005) destaca que: "os certificados digitais possuem prazos de validade: desse modo, uma determinada chave privada só pode ser utilizada para assinar um documento enquanto o certificado que dá validade à respectiva chave pública estiver válido. Além disso, o certificado pode ser suspenso – quando, por exemplo, pairarem dúvidas sobre o titular do certificado – ou revogado – nos casos de comprometimento da chave privada. Convém ressaltar, entretanto, que apesar de não poder mais se utilizar aquela chave privada para assinar um documento, as infra-estruturas devem estar preparadas para continuar validando os documentos assinados quando o certificado ainda era válido, ou seja, os certificados devem permanecer armazenados por um tempo longo o

suficiente para garantir a conferência das assinaturas digitais realizadas com as chaves privadas respectivas”.

## 2.15. ISO/IEC 27001:2005

Com a crescente preocupação em torno da CID (confidencialidade, integridade e disponibilidade da informação), tudo leva a crer que a próxima onda de certificações nas empresas será a da “gestão segura”. Tal como a ISO 9000 (gestão da qualidade) e a ISO 14000 (gestão ambiental), a segurança da informação ganhou sua própria norma: a ISO 27001. Lançada em outubro de 2005, ela se apóia em legislações internacionais de proteção de dados e sistemas, como a britânica BS-7799. Os requisitos vão desde manter a mesa limpa, sem documentos importantes expostos a olhares curiosos, até a elaboração de um “Plano de Continuidade de Negócio – PCN” capaz de garantir a operação da empresa em casos de ataque aos seus dados mais importantes.

Consultando-se o *site* <http://www.iso27001certificates.com/> em pode-se verificar a existência já de 16 empresas no Brasil certificadas pelas normas ISMS standard BS 7799 Part 2:2002 ou ISO/IEC 27001:2005 (a revisão da BS 7799 Part 2:2002) sendo elas:

Empresas no Brasil certificadas na BS 7799-2:2002 ou ISO/IEC 27001:2005

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
Atos Origin Brasil Ltda	Brazil	IS 98429	BSI	ISO/IEC 27001:2005
Axur Information Security	Brazil	IS 509742	BSI	ISO/IEC 27001:2005
Banco Matone S.A	Brazil	07502-2003-AIS-LDN-UKAS	DNV	BS 7799-2:2002
CIP Camara Interbancaria de Pagamentos	Brazil	IS 96934	BSI	ISO/IEC 27001:2005
Fucapi - Fundação Centro de Análise	Brazil	IS 504391	BSI	ISO/IEC 27001:2005
Modulo Security Solutions S.A	Brazil	0012-2005-AIS-OSL-NA	DNV	ISO/IEC 27001:2005
Módulo Security Solutions S/A	Brazil	IS 510466	BSI	ISO/IEC 27001:2005
Prodesp	Brazil	IS 512881	BSI	ISO/IEC 27001:2005
Promon Engenharia Ltda.	Brazil	IS 500248	BSI	ISO/IEC 27001:2005
Promon Tecnologia Ltda	Brazil	IS 500564	BSI	ISO/IEC 27001:2005

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
SAMARCO MINERAÇÃO S.A.	Brazil	07584-2005-AI-LDN-UKAS/Rev 1	DNV	ISO/IEC 27001:2005
SAMARCO MINERAÇÃO S/A	Brazil	07584-2005-AI-LDN-UKAS	DNV	BS 7799-2:2002
Serasa, São Paulo	Brazil	262326 IS	DQS GMBH	BS 7799-2:2002
Serviço Federal de Processamento de Dados - SERPRO	Brazil	00014-2006-AIS-OSL-NA	DNV	BS 7799-2:2002
Serviço Federal de Processamento de Dados - SERPRO	Brazil	IS 515421	BSI	ISO/IEC 27001:2005
Telefonica Empresas S/A	Brazil	IS 501039	BSI	BS 7799-2:2002
Tivit Tecnologia da Informacao S.A.	Brazil	00017-2006-AIS-OSL-NA	DNV	ISO/IEC 27001:2005
T-Systems Brazil	Brazil	336227 ISMS	DQS	ISO/IEC 27001:2005
UNISYS Global Outsourcing & Infrastructure Services (GOIS)/Maintenance Support Services (MSS)	Brazil	IS 97102	BSI	ISO/IEC 27001:2005

Fonte: <http://www.iso27001certificates.com/> em 03/09/2007.

“A publicação da ISO/IEC 27001:2005 é um grande acontecimento no mundo da segurança da informação, que tem sido ansiosamente aguardado”, diz Ted Humphreys, coordenador do grupo de trabalho responsável por gerenciar o desenvolvimento da norma. “É uma norma que toda organização ciente da importância da segurança deveria procurar implementar”.

A ISO/IEC 27001:2005 pode ser usada por um grande número de organizações (pequenas, médias e grandes) da maioria dos setores comerciais e industriais: finanças e seguros, telecomunicações, utilidades, varejo e manufatura, diversos setores de serviço, transportes, governo e muitos outros.

A implementação da ISO/IEC 27001:2005 reafirmará para os clientes e fornecedores que a segurança da informação está sendo levada a sério pelas organizações

com as quais eles fazem negócio, pois empregam processos de última geração para lidar com as ameaças e os riscos à segurança da informação.

Assim como outros importantes ativos empresariais, a informação é um ativo que agrega valor à organização e conseqüentemente precisa ser protegida. A segurança da informação protege a informação de um grande número de ameaças, a fim de garantir a continuidade dos negócios, minimizar danos e maximizar o retorno sobre os investimentos e as oportunidades de negócios.

A ISO/IEC 27001:2005 integra a abordagem baseada em processos das normas para sistemas de gestão da ISO (ISO 9001:2000 e ISO 14001:2004), incluindo o ciclo PDCA (planejamento, execução, verificação, ação) e o requisito de melhoria contínua.

A nova norma forma o par complementar com a ISO/IEC 17799:2005, também publicada recentemente, a qual é o “código de práticas” sobre a gestão da segurança da informação.

Até agora, as organizações que desejavam certificar seus Sistemas de Gestão da Segurança da Informação (SGSI) utilizavam a norma britânica BS 7799, parte 2. Agora, isso já é possível com a ISO/IEC 27001:2005, que é uma norma internacional.

## **2.16. *Presente e futuro digital***

O conhecimento está definitivamente condenado a ser armazenado em meios digitais. O papel utilizado por séculos como forma de retenção da sapiência humana está sendo substituído pelos arquivos digitais. Não faz muito tempo que toda família que tinha alguém na escola possuía em casa uma enciclopédia com vários volumes na estante. Livros que acumulavam o conhecimento de séculos de pesquisa e anos de trabalho para a sua confecção. Hoje, tais livros foram substituídos por enciclopédias digitais, tais como a Wikipedia ([www.wikipedia.com](http://www.wikipedia.com)), onde a informação é atualizada constantemente e acrescida de maneira infinita.

A digitalização caminha com tanta força que até mesmo o que há pouco tempo era impensável está se tornando realidade. O governo federal através do Decreto nº 6.022, de 22 de janeiro de 2007, instituiu a Sistema Público de Escrituração Digital – SPED. O Artigo 1º sumariza o seu significado: “O SPED é instrumento que unifica as atividades de

recepção, validação, armazenamento e autenticação de livros e documentos que integram a escrituração comercial e fiscal dos empresários e das sociedades empresárias, mediante fluxo único, computadorizado, de informações” (ver apêndice A na página LVI).

O SPED é mais um avanço na informatização da relação fisco-contribuinte consiste na modernização da sistemática atual do cumprimento das obrigações acessórias, transmitidas pelos contribuintes às administrações tributárias e aos órgãos fiscalizadores, utilizando-se da Certificação Digital para fins de assinatura dos documentos eletrônicos, garantindo assim a validade jurídica apenas na sua forma digital. O SPED:

- É composto por três grandes subprojetos: Escrituração Contábil Digital, Escrituração Fiscal Digital e a NF-e - Ambiente Nacional;
- Representa uma iniciativa integrada das administrações tributárias nas três esferas governamentais: federal, estadual e municipal;
- Mantém parceria com 16 instituições, entre órgãos públicos, conselhos de classe, associações e entidades civis, na construção conjunta do projeto;
- Firma Protocolos de Cooperação com 24 empresas do setor privado, participantes do projeto-piloto, objetivando o desenvolvimento e o disciplinamento dos trabalhos conjuntos;
- Possibilita, com as parcerias fisco-empresas, planejamento e identificação de soluções antecipadas no cumprimento das obrigações acessórias, em face às exigências a serem requeridas pelas administrações tributárias;
- Faz com que a efetiva participação dos contribuintes na definição dos meios de atendimento às obrigações tributárias acessórias exigidas pela legislação tributária contribua para aprimorar esses mecanismos e confira a esses instrumentos maior grau de legitimidade social; e
- Estabelece um novo tipo de relacionamento, baseado na transparência mútua, com reflexos positivos para toda a sociedade.

### **3. Metodologia**

De forma geral, os critérios utilizados para definir os tipos de pesquisa variam entre os diversos autores. A opção pela utilização da metodologia de estudo de caso com seleção de caso único foi devido aos conceitos e argumentos abaixo apresentados.

#### **3.1. *Pesquisa exploratória***

O objetivo principal da pesquisa exploratória é a busca pelo entendimento sobre a natureza geral de um problema. A pesquisa exploratória é tradicionalmente utilizada em áreas onde existe pouco conhecimento acumulado e sistematizado sobre o assunto a ser pesquisado. A pesquisa visa aprofundar questões a serem estudadas e ganhar maior conhecimento sobre um tema. Possui uma forma de investigação mais flexível e menos estruturada do que a realizada em uma pesquisa conclusiva devido a sua natureza de sondagem. Segundo Boyd e Westfall (1984), o estudo exploratório tem como principal objetivo encontrar idéias e novas relações para elaborar explicações prováveis. Uma vez que existem poucos estudos acadêmicos e científicos publicados sobre os aspectos de utilização do certificado digital para garantir a segurança da informação, tema deste trabalho, a opção pela adoção da pesquisa exploratória parece ser a mais adequada conforme o conceito exposto acima. Desta forma, a abordagem exploratória irá permitir o detalhamento do conhecimento sobre o assunto estudado, aumentando a sua compreensão através de uma investigação flexível.

De acordo com Yin (2001), a abordagem exploratória pode ser utilizada em qualquer um dos cinco tipos principais de estratégias de pesquisa: experimento, levantamento, análise de arquivos, pesquisa histórica e estudo de caso.

#### **3.2. *Estudo de caso***

Conforme Boyd e Westfall (1984), o método do caso é um estudo intensivo de um número pequeno de casos, que tem por objetivo a obtenção de uma compreensão das relações dos fatores em cada caso, independentemente do número de casos envolvidos. É

útil quando um problema envolve a inter-relação de vários fatores e quando for difícil compreender os fatores individuais sem considerá-los em suas relações com os outros. Através desta abordagem é possível o aparecimento de relações entre os fatores do caso e, que de outras formas, não poderiam ser descobertas.

O estudo de caso não é apenas um método de coleta de dados, mas sim, uma estratégia de pesquisa abrangente. Conforme a definição proposta por Yin (2001): “Um estudo de caso é uma investigação empírica que:

- Investiga um fenômeno contemporâneo dentro de seu contexto na vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos;
- Enfrenta uma situação em que o número de variáveis de interesse é muito maior do que o número de pontos de dados;
- Baseia-se em várias fontes de evidências necessitando de uma triangulação para a convergência dos dados;
- Beneficia-se do desenvolvimento de proposições teóricas prévias para conduzir a coleta e a análise dos dados.”.

A partir do conceito de estudo de caso proposto por Yin (2001), a utilização do método do caso como estratégia para guiar a realização deste trabalho justifica-se pelas seguintes razões:

- A gestão da segurança da informação é um fenômeno novo que ainda não está claramente definida;
- O estudo baseia-se em várias fontes de evidência, tais como: revisão da literatura de teorias de gestão da segurança da informação e entrevistas com gestores de segurança da informação das Unidades Administrativas da Receita Federal do Brasil na 7ª Região Fiscal.

A proposição teórica apresentada no capítulo de fundamentação teórica orientou a condução e análise do estudo de caso.

De acordo com os conceitos e as justificativas apresentados, a opção pela utilização do método do caso parece adequada para atingir os objetivos propostos pela pesquisa, quais

sejam, verificar se a utilização do *smartcard* resolveria o problema dos esquecimentos de contas e senhas, acabaria com as anotações de contas e senhas em papéis e também com o compartilhamento de contas por mais de um usuário, pelo menos com relação aos sistemas mais sensíveis a segurança da informação.

Entretanto, uma das principais críticas em relação à metodologia do estudo de caso é o fato de oferecer poucas bases para se fazer uma generalização científica ou estatística. De acordo com Yin (2001), uma vez que o objetivo dos estudos de caso é o de prover análises “generalizantes” e não “particularizantes”. Na generalização analítica o pesquisador procura generalizar um conjunto particular de resultados à uma teoria mais abrangente. Este trabalho não tem o objetivo da realização de generalizações estatísticas.

### **3.3. Seleção do Caso Único**

Segundo Yin (2001) o estudo de caso único é indicado quando um conjunto de condições, ou de fundamentos lógicos, está presente para justificar sua adoção:

- O estudo de caso representa o caso decisivo para testar uma teoria ou um conjunto de teorias e proposições bem formuladas sobre um determinado assunto;
- O caso representa um caso raro ou extremo, ou seja, possui características especiais e únicas que por si só merecem ser analisadas e documentadas;
- O caso é um caso revelador, ou seja, é analisável pelo pesquisador que tem uma oportunidade especial para observar e investigar um caso que é praticamente inacessível aos demais membros da comunidade científica;

Segundo Yin (2001), os resultados de um estudo de caso provavelmente serão mais convincentes e precisos quando baseados em fontes distintas de informação. Desta forma, para buscar maior riqueza de informações para a dissertação optou-se pela utilização das três formas de coletas de informações, determinando as seguintes três fases de coleta de dados:

- Estudo de dados secundários - na primeira fase da pesquisa foram utilizadas as fontes secundárias para aprofundar a revisão bibliográfica. Foram pesquisados livros, artigos de jornais e revistas, artigos científicos e demais

publicações que possibilitassem a obtenção de dados relevantes e atualizados sobre segurança da informação e sobre certificação digital;

- Entrevista com profissionais da empresa – neste período foram entrevistados os gestores de segurança das Unidades Administrativas (UAs) da 7ª região fiscal da Receita Federal do Brasil;
- Análise dos dados – Segundo Yin (2001), a análise dos dados, consiste em examinar, categorizar, classificar em tabelas ou recombina as evidências encontradas na pesquisa tendo em vista as proposições teóricas iniciais do estudo. Uma vez que a principal função do método do caso é a explicação sistemática dos fatos que ocorrem no contexto social e que se relacionam com uma multiplicidade de variáveis, os dados podem ser apresentados sob a forma de tabelas, quadros, gráficos e por meio de uma análise descritiva que os caracterizam.

## **4. Estudo de caso**

A Secretaria da Receita Federal do Brasil, instituída recentemente pelo decreto lei nº 11.457 de março de 2007 que unificou a Secretaria da Receita Federal com a Secretaria da Receita Previdenciária, tem a missão de prover o Estado de recursos para garantir o bem-estar social, prestar serviços de excelência à sociedade e prover segurança, confiança e facilitação para o comércio internacional. Seus principais valores são: respeito ao cidadão, integridade, lealdade com a Instituição, legalidade e profissionalismo. Sua visão de futuro é ser reconhecida como uma organização dotada de política moderna de gestão de pessoas que presta serviços de excelência. Almeja também ser referência nacional e internacional além de ser reconhecida como justa e sólida.

#### **4.1. A Secretaria da Receita Federal do Brasil (RFB)**

A Secretaria da Receita Federal do Brasil (RFB) tem como principais objetivos:

- Subsidiar a formulação da política tributária e de comércio exterior;
- Promover a integração da RFB com órgãos de Estado e organismos, nacionais e internacionais;
- Intensificar a atuação da RFB no combate ao crime organizado;
- Fortalecer a imagem institucional da RFB e promover a conscientização tributária do cidadão;
- Promover o atendimento de excelência ao contribuinte;
- Otimizar o controle e a cobrança do crédito tributário;
- Aprimorar a qualidade e a produtividade do trabalho fiscal;
- Aumentar a eficácia da vigilância e da repressão aos ilícitos aduaneiros;
- Simplificar, padronizar e agilizar o controle aduaneiro;
- Aumentar a eficiência e a eficácia no preparo, análise e julgamento dos processos administrativo-fiscais;
- Promover o aperfeiçoamento, a simplificação e a consolidação da legislação tributária federal e uniformizar a interpretação;
- Aperfeiçoar a política de Gestão de Pessoas na RFB;
- Aumentar a eficácia, a eficiência e a efetividade na gestão orçamentária, financeira e patrimonial e de mercadorias apreendidas;
- Aprimorar a política de gestão da informação e de infra-estrutura de tecnologia;
- Implementar gestão de excelência na RFB

Suas diretrizes institucionais para 2007 são:

- Concentração de esforços e recursos na efetiva implantação da Secretaria da Receita Federal do Brasil;
- Revisão e simplificação dos processos (procedimentos e legislação), com foco nas necessidades e no perfil dos contribuintes;

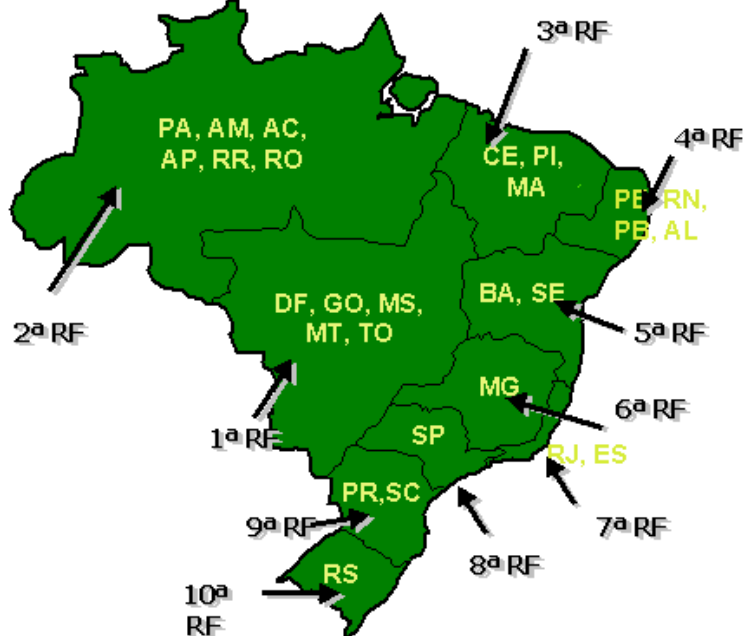
- Controle integral dos contribuintes sujeitos ao acompanhamento diferenciado;
- Liderança da RFB no processo de agilização do fluxo do comércio exterior, com segurança e controle;
- Aumentar a eficácia da recuperação do crédito tributário, favorecendo o aumento da presença fiscal, a agilização do julgamento de processos fiscais e a agilização da cobrança administrativa;
- Integração e cooperação da RFB com as demais Administrações Tributárias Nacionais;
- Ênfase na política de gestão de pessoas, como responsabilidade do conjunto de administradores, destacando a capacitação, a valorização e a motivação do servidor;
- Intensificação da interação com a sociedade, por meio da educação fiscal e da facilitação do cumprimento voluntário das obrigações tributárias;
- Intensificação das atividades de repressão aos ilícitos fiscais e aduaneiros.

#### ***4.1.1.Estrutura organizacional***

A Secretaria da RFB é composta por unidades centrais e unidades descentralizadas, distribuídas por todo o território nacional, abrangendo uma área de 8,5 milhões de quilômetros quadrados.

## Receita Federal do Brasil

BRASIL	
SRRF	10
DRF	97
DRP	7
DRJ	18
DEINF	2
DEAIN	1
DEFIS	2
DERAT	2
IRF	57
ALF	23
ARF	359
<b>TOTAL</b>	<b>578</b>



Legenda das siglas:

SRRF – SUPERINTENDÊNCIAS REGIONAIS DA RFB

DRF – DELEGACIAS DA RFB

DRP – DELEGACIAS DA RFB PREVIDENCIÁRIAS

DRJ – DELEGACIAS DA RFB DE JULGAMENTO

DEINF - DELEGACIAS ESPECIAIS DE INSTITUIÇÕES FINANCEIRAS

DEAIN - DELEGACIA ESPECIAL DE ASSUNTOS INTERNACIONAIS

DEFIS - DELEGACIAS DA RFB DE FISCALIZAÇÃO

DERAT - DELEGACIAS DA RFB DE ADMINISTRAÇÃO TRIBUTÁRIA

IRF - INSPETORIAS DA RFB

ALF - ALFÂNDEGAS DA RFB

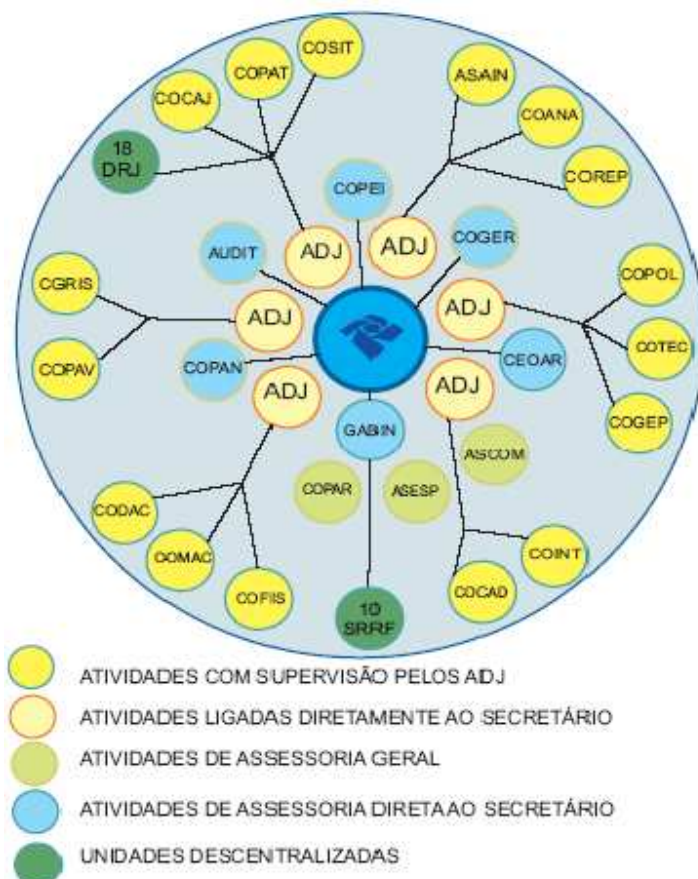
ARF - AGÊNCIAS DA RFB

## Quantitativo de unidades descentralizadas por Região Fiscal

	RF 01	RF 02	RF 03	RF 04	RF 05	RF 06	RF 07	RF 08	RF 09	RF 10	BRASIL
ALF	1	4	3	2	2		4	3	2	2	23
ARF	32	22	34	34	33	38	22	64	42	38	359
DEAIN								1			1
DEFIS							1	1			2
DEINF							1	1			2
DERAT							1	1			2
DRF	7	9	7	9	6	12	5	21	12	9	97
DRJ	2	1	1	1	1	2	2	4	2	2	18
DRP							3	4			7
IRF	6	16	1	4	3	1	2	2	10	12	57
SRRF	1	1	1	1	1	1	1	1	1	1	10
TOTAL	49	53	47	51	46	54	42	103	69	64	578

A Secretaria da Receita Federal do Brasil – RFB – é chefiada pelo Secretário Jorge Antônio Deher Rachid e 6(seis) Secretários Adjuntos sendo assessorados por diversas coordenações e ainda 3(três) adidâncias no exterior.

## Organograma da Receita Federal do Brasil



## **4.2. A Gestão da Segurança da Informação na RFB**

### **4.2.1. A Informação – fator de produção na RFB**

A RFB tem como seu principal fator de produção a informação. O modelo de arrecadação de tributos adotada no Brasil é do da declaração espontânea por parte do contribuinte que paga seus tributos durante o ano fiscal e faz uma declaração de ajuste anual acertando as contas com o Fisco. No caso da Pessoa Física (PF) é a Declaração do Imposto de Renda Pessoa Física (DIRPF) e no caso da Pessoa Jurídica (PJ) é a Declaração de Informações Econômico Fiscais da Pessoa Jurídica (DIPJ). As informações prestadas pelos contribuintes são armazenadas nos bancos de dados da Secretaria da Receita Federal do Brasil e comparadas com as diversas fontes de dados que a RFB dispõe para averiguar a veracidade das declarações. Como exemplo pode-se citar a Declaração de Imposto de Renda Retido na Fonte (DIRF) que as fontes pagadoras (PF e PJ) são obrigadas a entregar ao fisco. Assim, as informações das pessoas físicas prestadas nas DIRPF podem ser confrontadas com aquelas informadas na DIRF e com outras fontes prestadas por administradoras de cartões de crédito, cartórios de registro imobiliários, bancos, órgãos estaduais e federais de licenciamento de veículos automotores (carros, barcos, aviões etc) e outros. A título de exemplo, seguem algumas declarações que são entregues a RFB: Declaração de Operações com Cartões de Crédito (DECRED) que as operadoras de cartão de crédito são obrigadas a prestar para a RFB; Declaração de Informações sobre Atividade Imobiliária (DIMOB) que os cartórios precisam prestar a RFB.

### **4.2.2. Segurança da Informação na RFB**

A RFB regulamentou a utilização dos seus sistemas de informação através de Portaria SRF/Cotec Nº 45, de 27maio de 2004 que dispõe sobre a Segurança e o Controle de Acesso Lógico e Físico no Ambiente Informatizado da RFB. Esta portaria identifica quais são os agentes intervenientes e suas atribuições, quais sejam: Titular da Unidade Administrativa (TUA), Gestor de Segurança, Gerente de Ambiente Informatizado, Cadastrador, Administrador de Ambiente Informatizado, Operador de Conta e Técnico de Suporte. Prevê ainda que a área de Tecnologia e Segurança da Informação da RFB deve

prover a capacitação e o desenvolvimento permanentes dos agentes intervenientes elencados anteriormente com exceção do TUA. Para se garantir o princípio da segregação são vedadas acumulações de funções tal como Gestor de Segurança com qualquer outra. Como no serviço público só se pode fazer aquilo que é previsto em lei (diferentemente do setor privado que se pode fazer tudo aquilo que não é proibido por lei), também são descritas as competências de cada agente interveniente tais como a do Gestor de Segurança que tem que: promover de forma continuada programas de conscientização e treinamento em segurança da informação; participar dos processos de prospecção, desenvolvimento e homologação de hardware, software e outros produtos e serviços de informática; gerenciar a implantação e a aplicação das normas de segurança da informação; fiscalizar permanentemente e auditar periodicamente o cumprimento das normas de segurança; realizar trabalho de análise de risco e vulnerabilidades e propor as medidas corretivas cabíveis; orientar a execução das atividades dos agentes intervenientes e demais usuários nos aspectos relativos à segurança da informação; determinar ao cadastrador ou operador de conta competente o bloqueio e a exclusão de contas, fundamentando a solicitação; relatar à sua chefia imediata e ao gestor de segurança que o supervisiona as irregularidades e eventos de segurança relevantes do Ambiente Informatizado.

A portaria também versa sobre o acesso físico às instalações do ambiente informatizado da RFB, restringindo este acesso ao: Titular da UA em que estão instalados os Equipamentos Servidores; Chefe da área de tecnologia e segurança de informação nas UAs sob sua supervisão; Gestor de Segurança nas UAs sob sua supervisão; Gerente de Ambiente Informatizado nas UAs sob sua supervisão; Administrador de Ambiente Informatizado nas UAs onde presta serviços; Técnico de Suporte nas UAs onde presta serviços; visitante autorizado por algumas pessoas elencadas anteriormente e de acordo com os procedimentos previamente definidos. Há também a questão do controle de acesso lógico ao ambiente informatizado devendo ser realizado por intermédio de mecanismos e procedimentos tendo por finalidade: proteger as informações da RFB contra o uso não autorizado; auxiliar na detecção de violações de segurança; assegurar recuperação nas situações de falha; permitir contabilização de informações; monitorar as atividades realizadas, preservando no mínimo as informações relativas à identificação do usuário, local, data e horário.

Estabelece ainda que as contas de serviço e outras contas e senhas com privilégios administrativos são de uso exclusivo e de responsabilidade solidária dos Administradores de Ambiente Informatizado dos segmentos correspondentes. Constitui também que as senhas de setup são de uso exclusivo e de responsabilidade solidária dos Administradores de Ambiente Informatizado e dos Técnicos de Suporte.

Há a formalização do cadastramento inicial vinculando o usuário a uma conta pessoal e intransferível e esta vinculação se consubstancia com a assinatura do Termo de Responsabilidade. As solicitações de cadastramento, atualização, exclusão, habilitação, desabilitação, bloqueio e desbloqueio de usuários devem-se fazer por meio de aplicação específica que contemple criptografia e assinatura digital, mediante o uso de certificados digitais da Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil).

#### ***4.2.3. Analisando o risco na RFB***

As informações prestadas pelos contribuintes são protegidas pelo Sigilo Fiscal. A RFB poderá ser responsabilizada caso seja comprovado que tais informações venham a vazar dos bancos de dados da instituição. Por isso, a RFB confia seus dados ao Serviço Federal de Processamento de Dados - SERPRO, empresa certificada pela DNV na norma BS 7799-2:2002 e pela BSI na ISO/IEC 27001:2005. Além disso, criou uma estrutura de tecnologia e segurança da informação onde realizou concurso público específico para recrutamento de pessoal com conhecimento de Tecnologia da Informação para preencher as vagas abertas nesta nova estrutura. Quase todas as unidades administrativas da RFB atualmente possuem um Gestor de Segurança da Informação que tem como responsabilidade, entre outras descritas no tópico anterior, realizar o trabalho de análise de risco e vulnerabilidades e propor as medidas corretivas cabíveis evitando que ameaças explorem vulnerabilidades existentes provocando perdas de confidencialidade, integridade e/ou disponibilidade, causando, possivelmente, impactos nas atividades da instituição. Pois o tratamento contínuo do risco é de fundamental importância para que se obtenha informações mais precisas quanto aos pontos fracos dos seus sistemas, pessoas e ambiente podendo assim tratá-los de acordo com os melhores critérios definidos para o seu perfil.

#### **4.2.4. Política de Segurança da Informação na RFB**

O servidor da Secretaria da Receita Federal está obrigado ao cumprimento dos deveres impostos no ordenamento legal a todos os agentes públicos. Ademais, pela peculiaridade em envolver-se, essencialmente, na atividade de arrecadar parte da renda dos contribuintes, o agente fazendário deve ter cuidados adicionais no trato da coisa pública, na postura profissional e na discrição necessária ao desempenho de sua função. Neste contexto, a Secretaria da Receita Federal do Brasil necessita de mecanismos voltados à proteção das informações estratégicas de que dispõe por força legal. A principal ferramenta para se assegurar essa proteção institucional traduz-se na conscientização de seus servidores para a importância da atividade por eles desenvolvida e nos cuidados que devem reservar, tanto no desenvolvimento de suas tarefas, quanto na segurança dos objetos físicos, informatizados ou cognitivos a que têm acesso. Com este escopo é que foi criado o Manual de Segurança Institucional da Secretaria da Receita Federal (MSI), instrumento de orientação ao servidor da Receita Federal no desempenho de suas atribuições legais. Constitui-se em iniciativa na busca do contínuo fortalecimento institucional da organização, por meio do aperfeiçoamento e atualização permanentes dos procedimentos e das recomendações normativas.

O MSI apresenta as regras e recomendações que estimulam a conscientização do corpo funcional da Receita Federal quanto aos riscos decorrentes de ações ou interesses externos e internos contra a instituição e seus servidores e à necessidade de salvaguardar conhecimentos e dados protegidos pelo sigilo fiscal.

Ele envolve medidas destinadas a prevenir e obstruir ações que possam causar danos sobre: pessoal; documentação; comunicações; sistemas de Informação; e áreas e instalações.

Abaixo segue a orientação legal (leis, decretos e portarias) que baseiam o MSI:

Lei nº 8.112, de 11 de dezembro de 1990 que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

Lei No 9.983, de 14 de julho de 2000 que altera o Código Penal para incluir crimes praticados em Sistemas de Informação da Administração Pública Federal;

Lei No 8.159, de 8 de janeiro 1991 que dispõe sobre a política nacional de arquivos públicos e privados;

Decreto No 3.505, de 13 de junho de 2000 que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

Decreto Nº 4.553, de 27 de dezembro de 2002 que dispõe sobre a Classificação de Informações na Administração Pública Federal;

Decreto Nº 4.073, de 3 de janeiro de 2002 que regulamenta a Lei no 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

Portaria SRF no 1.103, de 30 de outubro de 2006 que regulamenta a geração, tratamento e guarda de registros de eventos (logs) no ambiente informatizado da Secretaria da Receita Federal;

Portaria SRF Nº 609, de 07 de abril de 2000 que dispõe sobre a extração de dados armazenados nas bases de dados em uso na SRF;

Portaria 66, de 20 de outubro de 2003 que regulamenta o uso de programas de computador de gerenciamento da rede corporativa na SRF, Backup e Antivírus;

Portaria SRF Nº 450, de 28 de abril de 2004 que dispõe sobre a Política de Segurança da Informação no âmbito da Secretaria da Receita Federal;

Portaria SRF/Cotec Nº 45, de 27 de maio de 2004 que dispõe sobre a Segurança e o Controle de Acesso Lógico e Físico nos Ambientes Cliente/Servidor da Secretaria da Receita Federal – SRF;

Portaria RFB/Cotec Nº 65, de 27 de outubro de 2005 que dispõe sobre utilização de Certificados Digitais e-CPF, no âmbito interno, pelos funcionários da Receita Federal do Brasil – RFB.

#### ***4.2.5. Classificação da Informação na RFB***

O Decreto Nº 4.553, de 27 de dezembro de 2002, dispõe sobre a Classificação de Informações na Administração Pública Federal. Os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos. O decreto instrui, por exemplo, para se classificar como ultra-secreto os dados referentes: à soberania e à integridade territorial nacional, aos planos e operações militares, às relações internacionais; a projetos de pesquisa e desenvolvimento

científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado. O Decreto informa também as competências para a classificação da informação. Por exemplo, são competentes para se classificar como ultra-secreto as seguintes autoridades: Presidente da República; Vice-Presidente da República; Ministros de Estado e autoridades com as mesmas prerrogativas; Comandantes da Marinha, do Exército e da Aeronáutica; Chefes de Missões Diplomáticas e Consulares permanentes no exterior e, excepcionalmente, esta competência pode ser delegada pela autoridade responsável a agente público em missão no exterior.

Outra informação importante é o tempo que o dado permanecerá com a classificação informada, pois como se sabe ela perde valor com o passar do tempo. O Decreto dispõe, por exemplo, que a informação classificada como ultra-secreta poderá permanecer assim por até trinta anos podendo ser prorrogada uma vez, por igual período, pela autoridade responsável pela classificação ou autoridade hierarquicamente superior competente para dispor sobre a matéria.

Não menos importante é o registro de toda a operação com o dado sigiloso. O Decreto, na Seção V - Do Registro, da Tramitação e da Guarda - dispõe sobre os cuidados necessários para se garantir o segredo da informação.

A RFB como órgão da Administração Pública Federal segue a mencionada lei na sua íntegra. Como exemplo, pode-se citar as diversas operações especiais que tem ocorrido pelo Brasil organizadas pela Coordenação de Repressão ao Contrabando e Descaminho (COREP). Todos os memorandos destas operações que versam sobre estas operações são tratados de forma sigilosa até o momento da ação de busca e apreensão, onde normalmente a imprensa, e por conseguinte, a população em geral tem conhecimento das operações.

#### **4.2.6. Recursos Humanos na RFB**

Além de se testar os conhecimentos necessários à atividade que será exercida na instituição, através de concurso público, no momento em que convocados para matrícula no Programa de Formação, os candidatos aprovados e classificados deverão apresentar, os documentos a seguir relacionados, indispensáveis à sindicância de vida pregressa:

a) certidão dos setores de distribuição dos foros criminais da Justiça Federal, Estadual, Militar e Eleitoral dos lugares em que tenha residido o candidato nos últimos 5 (cinco) anos;

b) declaração firmada pelo candidato, da qual conste não haver sofrido condenação definitiva por crime ou contravenção, nem penalidade disciplinar de demissão, no exercício de cargo ou de destituição de função pública;

c) declaração do órgão público, ao qual esteja vinculado o candidato à data da matrícula na Segunda Etapa, de não estar respondendo a procedimento administrativo disciplinar (sindicância ou inquérito) nem ter sofrido penalidade administrativa de suspensão.

d) folha de antecedentes expedida pela Polícia do Distrito Federal ou dos Estados onde residiu o candidato, nos últimos 5 (cinco) anos, expedida, no máximo, há 6 (seis ) meses.

Passando por esta fase, inicia-se o Programa de Formação onde os candidatos são instruídos com os conhecimentos necessários ao exercício do cargo inclusive sendo informados das atividades da Corregedoria do Órgão que tem como principal função gerenciar e executar as atividades de investigação disciplinar e demais atividades de correição e promover ações preventivas e repressivas relativas à ética e à disciplina funcionais dos servidores lotados ou em exercício na RFB . São também informados sobre os Processos Administrativos Disciplinares (PAD) que estão sujeitos caso não exerçam suas funções conforme ordenamento legal. São apresentados também ao Manual de Segurança Institucional (MSI) onde são tratados aspectos de segurança: do pessoal, da documentação, das comunicações, dos sistemas informáticos e das áreas e instalações. Além disso, regularmente são ministradas palestras a respeito do MSI mantendo assim na memória do servidor a necessidade de se preservar a segurança na RFB.

O princípio da segregação é amplamente aplicado na instituição até mesmo no que tange a contratação de serviços externos. Por exemplo, no projeto de implantação da rede de computadores foi contratada uma empresa para realizar o pré-projeto que obrigatoriamente foi diferente daquela que realizou o projeto que também teve que ser diferente daquela que implantou o projeto. Mantendo a lisura no processo e evitando assim erros e favorecimentos indevidos.

#### ***4.2.7.A Segurança Física na RFB***

O Serviço de Processamento de Dados do Governo Federal (SERPRO) - empresa pública que presta serviços em Tecnologia da Informação e Comunicações para o setor público, inclusive para a RFB - buscou a sua certificação junto a DNV segundo a norma BS 7799-2:2002 e posteriormente junto a BSI na ISO/IEC 27001:2005, dando maior proteção aos dados custodiados pela RFB.

Os computadores chamados Servidores (não confundir com as pessoas que trabalham para o governo) localizados na RFB são centralizados numa sala escura, onde só podem entrar pessoas autorizadas, após passar por áreas também restritas e monitoradas. Os acessos são registrados e devem ser motivados pelo serviço.

Com relação à segurança predial só se permite a entrada de pessoas devidamente identificadas na portaria. Os funcionários precisam portar crachás de identificação assim como os visitantes identificados no corredor de entrada.

Todos os andares possuem câmeras de circuito fechado de TV que permitem a identificação das pessoas caso haja alguma irregularidade. Estas imagens ficam armazenadas em formato digital para serem acessadas quando necessário.

#### ***4.2.8. Segurança de Equipamentos Móveis na RFB***

A violência urbana pela qual é acometida a sociedade brasileira não é novidade e até a presente data não se tem nenhum sinal claro de que o problema será resolvido a curto ou médio prazo. Por isso, é extremamente importante a adoção de medidas que visem a garantia do sigilo das informações contidas em equipamentos móveis caso estes venham a ser extraviados. Recentemente foi implementado nos notebooks da RFB um local de

armazenamento de arquivos (pasta) onde todos os dados ali guardados são criptografados de forma transparente para o usuário. Caso o computador portátil venha a ser subtraído do seu usuário, os dados que estiverem nesta pasta não poderão ser lidos, nem mesmo pelo administrador do computador. As unidades de armazenamento portáteis conhecidas como *pendrive* também possuem um software de criptografia que deve ser usado quando ali forem transportadas informações protegidas pelo sigilo fiscal. Desta forma, o desaparecimento de um equipamento móvel trará prejuízo apenas com relação ao valor do hardware e não ao conteúdo ali guardado. Para que estas medidas funcionem em sua plenitude os detentores destes equipamentos precisam passar pelo departamento de Tecnologia e Segurança da Informação periodicamente para atualizar as medidas de segurança que não podem ser feitas remotamente.

#### ***4.2.9. Descarte de equipamentos e de documentos na RFB***

No mundo atual com dispositivos cada vez menores e mais potentes, tais como os telefones inteligentes (smartphones) que filmam com qualidade de filmadora digital com 30 quadros por segundo e definição de 640 colunas por 480 linhas (idêntico a definição dos DVDs), fotografam com flash e definição de 5Mpixels, gravam horas de conversação, armazenam Gigabytes de informação funcionando como mídia removível (tipo pendrive), as informações estão bem mais suscetíveis de serem copiadas sem autorização. Qualquer um com um aparelho deste em mãos pode registrar tudo que estiver fisicamente ao seu alcance. Por isso, os documentos descartados na RFB devem ser todos triturados em equipamentos apropriados. Nenhuma informação sigilosa pode ser descartada sem as devidas ações para efetivamente eliminá-las não deixando nenhuma hipótese para que ela seja recuperada. Na RFB, há a instrução de se usar trituradoras de papel para os documentos físicos e o software ERASER para os arquivos digitais. Ao contrário do que muitos pensam, os arquivos digitais quando saem da lixeira do sistema operacional continuam a existir na mídia (disco rígido, pendrive etc). Podendo ainda ser recuperado. Para que eles sejam efetivamente eliminados há a necessidade de se usar um software específico para isso.

#### **4.2.10. Controle de acesso na RFB.**

Recentemente, mais precisamente no dia 4 de dezembro de 2007, foi veiculada uma matéria no Jornal Nacional na TV Globo mostrando a fragilidade do sistema de segurança pública do estado do Rio Grande do Sul. Nela um policial corrupto passa informações sigilosas a um foragido da justiça e também a um detetive particular. O repórter da TV encomenda os dados sigilosos do ministro da Justiça Tarso Genro e foi atendido em menos de 24h com dados verdadeiros conforme verificado pela própria polícia civil. O Secretário de Segurança Pública do Estado do RS, somente após o conhecimento dos fatos solicitou que todas as senhas fossem alteradas.

Os sistemas corporativos com dados sigilosos da RFB obrigam os seus usuários a mudarem as senhas periodicamente. Este simples fato evita que mesmo que alguém consiga descobrir a senha de um usuário, este perderia esta vantagem em pouco tempo quando da obrigatoriedade da mudança de senha. Caso a senha seja alterada pelo contraventor o usuário autorizado vai ao cadastrador do sistema solicitar nova senha. Além disso, todos os sistemas possuem logs para auditoria coibindo assim atividades ilícitas. Atualmente a maioria dos sistemas já exige o uso do cartão inteligente (*smartcard*), dispositivo que implementa a Certificação Digital. Dificultando ainda mais ações ilegais, pois além de conhecer a senha é necessário o porte do *smartcard*. Num futuro breve, todos os sistemas da RFB, tanto os corporativos quanto os operacionais, exigirão o uso da Certificação Digital.

Existe na RFB uma política de desenvolvimento de software (programa de computadores) que exige que atenda aos requisitos mínimos de segurança para garantir a confidencialidade, integridade e disponibilidade. Desde 2004, a Portaria SRF Nº 450 ,de 28 de abril, em seu artigo primeiro diz:

“A Política de Segurança da Informação, no âmbito da Secretaria da Receita Federal (SRF), tem como pressuposto a garantia da confidencialidade, integridade e disponibilidade dos ativos de informação”.

O SERPRO, principal prestador de serviço de Tecnologia da Informação e Comunicação (TIC) da RFB criou o Processo SERPRO de Desenvolvimento de Soluções – PSDS com o objetivo de padronizar e documentar as atividades realizadas para conceber

soluções de TIC para seus clientes. Para garantir a institucionalização e a melhoria contínua do PSDS, em consonância com os objetivos e as metas empresariais e em conformidade com as melhores práticas de desenvolvimento e manutenção de software consolidadas no mercado, foi criado o Programa SERPRO de Melhoria do Desenvolvimento de Soluções – PSMDS. O PSDS define: O que deve ser feito; Como deve ser feito; Quando deve ser feito; Por quem deve ser feito; e Com o que deve ser feito. Todos os sistemas desenvolvidos para a RFB devem garantir a confidencialidade, integridade e disponibilidade, além da legalidade e da irretratabilidade (não-repúdio).

#### **4.2.11. *Certificação digital na RFB***

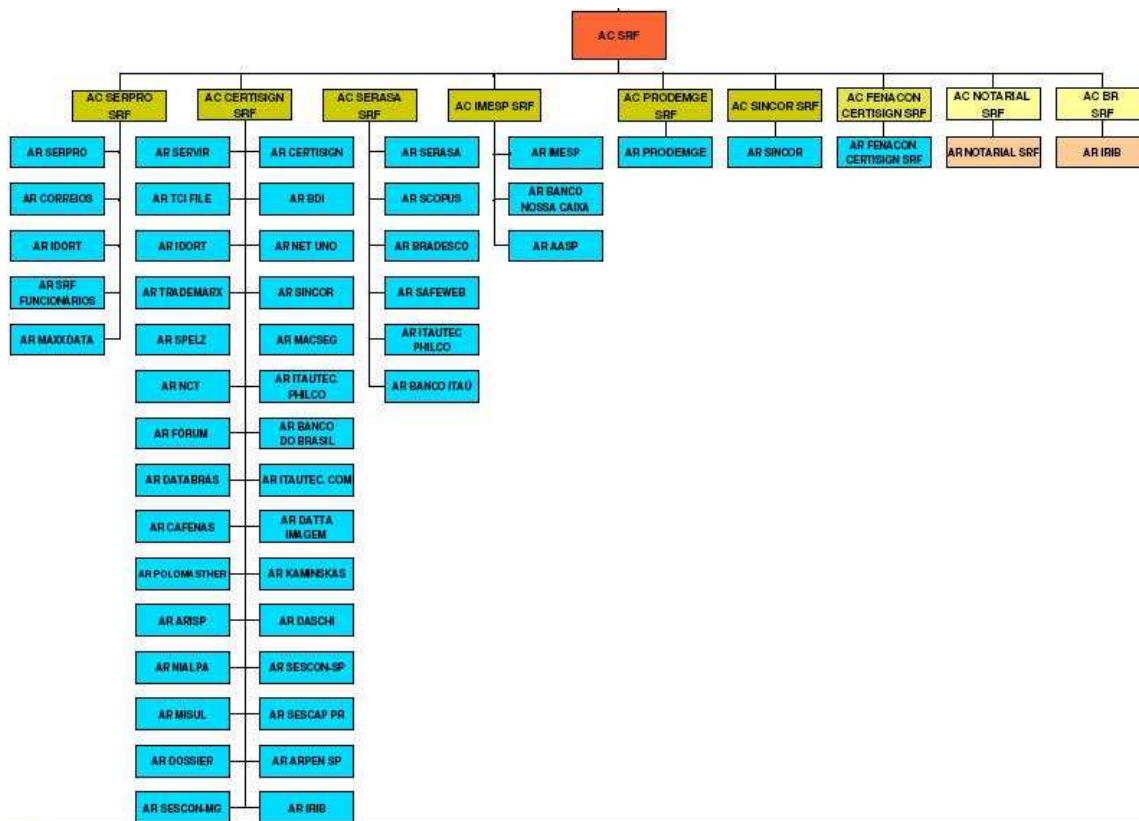
A RFB tem sido pioneira na utilização e divulgação da certificação digital. Desde 2005, várias empresas já são obrigadas a trabalhar com o um certificado digital, como pode ser conferido na página:

<http://www.receita.fazenda.gov.br/Pessoafisica/ReceitaNet/EntregaCertfDigital.htm#Entrega%20Obrigatória%20Com%20Certificação%20Digital> em 05/12/2007.

A Receita Federal do Brasil adotou o Certificado Digital para que os serviços protegidos por sigilo fiscal também possam ser atendidos por meio de sua página na Internet. Esses serviços utilizam a tecnologia que certifica a autenticidade dos emissores e destinatários dos documentos eletrônicos, assegurando sua privacidade e inviolabilidade. Com essa garantia, o contribuinte pode, entre outras coisas, obter cópia de declarações, cópia de pagamentos, realizar retificação de pagamentos, negociar parcelamento, pesquisar sua situação fiscal, realizar transações relativas ao Sistema Integrado de Comércio Exterior, além de alterar seus dados cadastrais. A RFB continua trabalhando para ampliar o universo de serviços prestados por meio de certificação digital. Cada vez mais serviços serão incluídos no Centro de Atendimento Virtual, para que o contribuinte possa ter a facilidade de ser atendido em sua casa ou escritório com a garantia da informação das unidades da Receita Federal.

A AC-SRF (Autoridade Certificadora Secretaria da Receita Federal, atual Receita Federal do Brasil) faz parte da Infra-estrutura de Chaves Públicas do Brasil – ICP Brasil estando abaixo da AC-Raiz (Instituto Nacional de Tecnologia da Informação). Abaixo desta estrutura estão várias outras como se pode ver na figura abaixo:

Estrutura da AC-SRF abaixo da AC-Raiz



Fonte: [http://www.iti.br/twiki/pub/Certificacao/Estruturalcp/Estrutura\\_completa.pdf](http://www.iti.br/twiki/pub/Certificacao/Estruturalcp/Estrutura_completa.pdf) em 5/12/2007.

As Autoridades de Registro (AR) são aquelas que recebem fisicamente os contribuintes e emitem os certificados digitais caso eles portem consigo os documentos necessários para a emissão do documento digital.

## 5. Discussão dos resultados

As entrevistas realizadas com os gestores de segurança da informação só confirmaram o que treinamentos, revistas, livros, palestras, artigos, monografias e dissertações na área de Gestão da Segurança da Informação informam: o elo mais fraco na segurança da informação é o Ser Humano. Leis, Instruções Normativas, Portarias e Notas Técnicas foram criadas visando implementar regras e procedimentos para se garantir a

Segurança da Informação no âmbito da Administração Pública Federal. Foram realizados na RFB diversos investimentos na aquisição de hardware – equipamentos - e software – programas – para a implementação da Segurança da Informação. Outras medidas tomadas incluem as palestras de conscientização da Política de Segurança da Informação e o Manual de Segurança Institucional, além da divulgação de cartazes sobre o assunto e uma página inicial no navegador da Internet de todas as estações com diversas mensagens sobre o assunto. Este material instrui sobre os problemas atuais relativos à segurança aos quais estão sujeitos os usuários de sistemas informáticos, deixando bem claro que as senhas não devem ser escritas, pois elas correm o risco de serem interceptadas gerando prejuízos para a instituição e para o usuário.

A principal medida para garantir a Segurança da Informação foi a implantação dos Smart Cards – Cartões Inteligentes – implementando a Certificação Digital no ambiente informatizado a Receita Federal do Brasil. Atualmente quase a totalidade dos usuários da RFB só consegue acessar o sistema operacional (o computador) utilizando o cartão inteligente. A previsão é que 100% dos usuários possuam a certificação digital em 2008 permitindo assim a implementação da certificação digital em toda a Receita Federal do Brasil.

Outro projeto que vem sendo implementado é a alteração dos sistemas corporativos, aqueles específicos das atividades da instituição. Estes programas estão sendo modificados de forma a permitir o acesso as suas bases de dados – informações – somente pelos usuários certificados – aqueles que possuem o cartão inteligente.

Para se coibir abusos, estão sendo implementadas ferramentas de bloqueio de acesso a páginas na Internet com conteúdo sexual ou esportivo. Existe a campanha de conscientização que informa ao usuário que o acesso a Grande Rede é compartilhado e por isso o seu uso é somente para fins profissionais, não a sobrecarregando com acessos particulares.

Há também a política de mesa limpa. Nela, os servidores são instruídos a não deixarem sobre a mesa os documentos físicos (papeis) ou digitais (mídias), principalmente aqueles protegidos pelo sigilo fiscal.

## 6. Conclusão

No século XXI, com a convergência digital, não se imagina a vida sem a utilização de um computador. Hoje se faz quase todas as operações bancárias sem se sair de casa; equipes de trabalhos geograficamente espalhadas podem trabalhar em um mesmo projeto como se na mesma sala estivessem; a telefonia saiu da exclusividade das concessionárias e passou a concorrer com a grande rede, através da tecnologia voz sobre o protocolo IP (VOIP); fotografias são enviadas diretamente do local onde são feitas para a redação dos jornais; contratos são assinados digitalmente; declarações de imposto de renda são feitas pela Internet; sistemas de segurança em tempo real utilizam a rede de computadores; todos os tipos de mensagens são trocados entre as pessoas etc.

Com o constante aumento da utilização de meios digitais para a realização de negócios faz-se necessária a utilização de mecanismos que identifiquem, de forma inequívoca, os envolvidos na transação, garantindo o sigilo e a inteireza da operação. A Certificação Digital será primordial para a confidencialidade, integridade e disponibilidade das informações, garantindo ainda o não-repúdio e a legalidade. Hoje no Brasil já estão disponíveis serviços prestados pelo Banco do Brasil e Receita Federal do Brasil. Estas instituições criaram sistemas e os colocaram na Internet de forma que os usuários possam utilizá-los remotamente garantindo a sua identificação de forma inconfundível. Para isso precisam garantir aos sistemas a sua identificação com a utilização do Certificado Digital (CD) que para ser adquirido, o seu interessado precisa ir pessoalmente a uma Autoridade de Registro (AR) com documentos originais e cópias além de fotos atuais. Esta AR solicita então a Autoridade Certificadora (AC) a emissão do CD. Este documento eletrônico servirá de identificação digital nas transações pela Internet.

Com o Certificado Digital, além dos serviços já prestados pelas instituições citadas anteriormente, diversas outras funcionalidades serão oferecidas pela Grande Rede. Há alguns anos já existe no Brasil a votação eletrônica para a escolha dos representantes do povo: vereadores, prefeitos, deputados, governadores, senadores e presidente. Num futuro não muito distante esta votação poderá ser feita pela Internet com a utilização da Certificação Digital acrescida de outras medidas, tal como identificação biométrica, para se evitar o Coronelismo com o seu curral eleitoral. Quem sabe a Certificação Digital poderá

inclusive acabar com a estrutura atual de votação no Congresso Nacional, onde as leis que mudam a vida do cidadão são votadas pelos Deputados eleitos para representar a vontade do povo de sua região. Vemos, não é de hoje, que muitas vezes estas votações são realizadas baseadas em acordos entre os congressistas visando os interesses partidários e não o da população que os elegeram, tal como o caso recente da CPMF. Estas leis poderão ser apresentadas a população que terá um prazo definido para ler, discutir, propor alterações ou votar, de acordo com seu próprio interesse.

Em fim, a Certificação Digital trará segurança para as operações digitais. Como o cartão inteligente (*smartcard*) será usado para todas as operações que necessitem a autenticação do usuário, o mesmo não precisará mais fazer anotações das diversas identificações e senhas que são necessárias sem a utilização do documento eletrônico. Permitirá ainda o aumento dos recursos a serem oferecidos pela Internet viabilizando operações antes restritas a presença física dos envolvidos, principalmente onde há a necessidade da assinatura do usuário.

## **7. Limitações**

São diversas as limitações desta dissertação, visto que o assunto é bastante complexo e pouco explorado. Uma das limitações que merece destaque é o fato do estudo de caso ser único, fazendo com que a análise do caso se restrinja somente à situação encontrada na 7ª Região Fiscal da Secretaria da Receita Federal do Brasil, mais especificamente na Unidades Administrativas localizadas no Palácio da Fazenda: DIFIS, DERAT, IRF, DRJ, SRRF. Portanto, não pode ser ampliada para as outras instituições de forma geral. O uso do caso único inviabiliza uma generalização estatística das conclusões.

Outra limitação foi o a tendência geral da concentração das informações obtidas nas entrevistas com o pessoal da área de segurança da informação. Este viés é devido ao assunto específico, uma vez que, ao se tratar apenas das questões referentes a segurança da informação, somente esta área possuía condições para respondê-las. Para atenuar esta limitação, foi utilizado também como fonte de evidências a observação pessoal e o exame de documentos e relatórios externos.

## 8. Sugestões para novas ações

A demanda por Segurança da Informação está bastante ampliada e por isso é muito importante que todos os aspectos desta nova área do conhecimento sejam bem explorados e compreendidos pelos profissionais da área de gestão da segurança da informação.

A tecnologia atualmente empregada para a implementação do par de chaves pública e privada é a RSA que trabalha com números primos de grandes valores onde com a tecnologia atual de computação fica inviável o processamento para se decodificá-los. Porém, com a promessa da implementação da computação quântica multiplicando  $n$  vezes a capacidade de processamento atual, este cálculo passaria a ser factível e quebraria a segurança atualmente empregada pela ICP-Brasil. É interessante que novas pesquisas sejam feitas para se identificar novas tecnologias para se manter a segurança da Certificação Digital.

Outro ponto a ser colocado é a implementação de scanners. Atualmente a tecnologia de identificação biométrica está se consolidando de forma que em pouco tempo será viável a implementação de equipamentos com esta tecnologia em larga escala permitindo assim os três fatores importantes na identificação do usuário: o que se conhece (senha), o que se possui (cartão inteligente) e a característica que se tem (identificação biométrica). Com a verificação destes três fatores, fica praticamente impossível que o acesso às informações seja feita por outra pessoa que não aquela que possui permissão para tal.

Atualmente, nos Estados Unidos, ao se entrar no país, os visitantes são cadastrados num sistema informático inclusive com o arquivamento da fotografia digital e da impressão digital digitalizada no desembarque nos aeroportos internacionais. Nos parques temáticos da Disney, a utilização da tecnologia de identificação biométrica foi implantada na simples operação de aluguel de armários para armazenamento de artigos pessoais. Lá o visitante antes de participar de uma atração “radical” precisa guardar os seus pertences nestes armários. A forma de identificação para reabrir o armário é através de leitor de impressão digital confirmando que a pessoa que deixou os pertences pessoais é a mesma que está solicitando a abertura do compartimento. Para finalizar há ainda o sistema

de identificação facial usada pela Royal Caribbean para a identificação dos passageiros que entram e saem dos seus navios. Através desta tecnologia os passageiros que embarcam num cruzeiro são registrados no porto de partida. A partir daí, todas as vezes que ele entra ou sai do navio a imagem registrada da sua face é confrontada automaticamente e digitalmente com aquela do cadastro de forma rápida e precisa.

## 9. Bibliografia

ALECRIM, Emerson. **Criptografia**. Infowester, 2005

<http://www.infowester.com/criptografia.php> em 30/08/2007.

ALVES, Gustavo Alberto. **Segurança da Informação: uma visão inovadora da gestão**. Rio de Janeiro: Ciência Moderna, 2006

BORTOLUZZI, Fabrício. **Estratégias de Segurança**. 2001, Monografia (Curso de Ciência da Computação) – Universidade do Vale do Itajaí, Itajaí.

BOYD, H; WESTFALL, R.; **Pesquisa Mercadológica – Textos e Casos**; 6ª Edição, Rio de Janeiro, Editora Getúlio Vargas, 1984.

CACIATO, Luciano Eduardo. **Gerenciamento da Segurança de Informação em Redes de Computadores e a Aplicação da Norma ISO/IEC 17799:2001**. 2004, Monografia (Curso de Análise de Sistemas) – PUC-Campinas, Campinas.

CALHEIROS, Rosenberg Faria. **Segurança de Informações nas Empresas: uma prioridade corporativa**. 2002, Trabalho de conclusão de curso (Curso de Biblioteconomia) – Escola de Biblioteconomia da Universidade do Rio de Janeiro, Rio de Janeiro.

CALHEIROS, Rosenberg Faria. **Segurança de Informações: uma questão estratégica**. 2004, Monografia (Curso de Pós-Graduação “Lato Sensu” em Gestão Estratégica e Qualidade) – Universidade Cândido Mendes, Rio de Janeiro.

FIGUEIREDO, Leonardo Soares. **Segurança da Tecnologia da Informação**. 2001, Monografia (Curso de Ciência da Computação) – Universidade Federal de Minas Gerais, Governador Valadares.

FIGUEIREDO, Leonardo Soares. **Segurança da Tecnologia da Informação**. 2002, Monografia (Pós-graduação em rede de telecomunicações) - 2002

FIGUEIREDO, Márcio Edmar Girard; DINIZ, Palmenas Costa; COROA, Sérgio Vinícius. **Segurança em Redes sem Fio Utilizando VPN Baseada em SSL**. 2005, Trabalho de Conclusão de Curso (Curso de Ciência da Computação) – Universidade da Amazônia – UNAMA, Belém.

FREITAS, Marco Antonio Diniz. **Análise da segurança da informação em ambientes corporativos**. 2002, Monografia (Curso de Engenharia) - Faculdade de Engenharia de Sorocaba – FACENS, Sorocaba.

FURTADO, Vasco. **Tecnologia e Gestão da Informação na Segurança Pública**. Rio de Janeiro: Garamond, 2002.

HOUAISS, A. **Dicionário Eletrônico da Língua Portuguesa**. São Paulo: Objetiva, 2001.

LACORTE, Christiano Vítor de Campos. **A Validade Jurídica do Documento Digital**. 2005, Artigo, Brasília.

LEMONS, Aline Moraes. **Política de Segurança da Informação**. 2001, Monografia (Curso de Administração) – UNESA – Universidade Estácio de Sá, Rio de Janeiro – RJ.

MAIOR, Alex de Oliveira Barros; SANTOS, Fábio Antonio dos; LACQUA, Sabrina Cristiane Dal. **Gestão da Segurança da Informação**. 2006, Monografia (Curso Engenharia da Computação) – FGP – Faculdade Gennari & Peartree, Pederneira - SP.

MELLO, Denis Vinícius de. **Resenha Segurança da Informação**. 2006, (Curso de Gestão da Tecnologia da Informação)

MENEZES, Josué das Chagas. **Gestão da Segurança da Informação**. Leme: Mizuno, 2006.

NETO, Cláudio de Lucena. **Segurança da Informação Corporativa: aspectos e implicações jurídicas**. 2003, Monografia (Curso de Direito) – Universidade Estadual da Paraíba, Campina Grande.

PEIXOTO, Mário César. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PEIXOTO, Mário César. **Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações**. 2004, Monografia (Curso de Ciência da Computação) - Centro Universitário do Triângulo – Unitri, Uberlândia.

RAMOS, Anderson; BASTOS, Alberto; LYRA, Alexandre; ANDRUCIOLI, Alexandre; AFFONSO, Carlos; POGGI, Eduardo; PINTO, Elaine; BLUM, Renato; ALEVATE, William; MARINHO, Zilta. **Guia Oficial para Formação de Gestores em Segurança da Informação – volume 1**. Porto Alegre: Editora Zouk, 2006.

RAMOS, Anderson; ANDRUCIOLI, Alexandre; SOUZA, Alexandre Domingos de; VARGAS, Alexandre; MICHELLIS, Denis; GALVÃO, Márcio; HASHIMOTO, Rafael; GIORGI, Ricardo; AGIA, Rodrigo. **Guia Oficial para Formação de Gestores em Segurança da Informação – volume 2**. Porto Alegre: Editora Zouk, 2007.

SANTOS, Luciano Alves Lunguinho. **O Impacto da Engenharia Social na Segurança da Informação**. 2004, Monografia (curso de Pós-Graduação em redes de computadores) – Universidade Tiradentes, Aracaju.

SELEGUIM, Guilherme Cestarolli. **Segurança da Informação: perigos do mundo virtual**. ????, Monografia (Curso de Análise de Sistemas) – PUC-Campinas, Campinas.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

VERGARA, Sylvia Constant. **Projetos e Relatórios de Pesquisa em Administração**. São Paulo: Atlas 2006.

YIN, R.; **Estudo de Caso – Planejamento e Métodos**; Bookman, 2001.

[http://www.certisign.com.br/certinews/banco\\_noticias/2007/06/tudo-sobre-certificacao-digital/](http://www.certisign.com.br/certinews/banco_noticias/2007/06/tudo-sobre-certificacao-digital/)

## Glossário

**Acesso imotivado:** aquele realizado para fins estranhos às necessidades de serviço;

**Acesso lógico:** operação de consulta ou de manutenção de dados e informações de um sistema informatizado;

**Ambiente de desenvolvimento:** conjunto de recursos utilizados para construir, testar e manter software;

**Ambiente de homologação:** conjunto de recursos utilizados para verificar se um software ou qualquer outro ativo de informação está em conformidade com sua especificação e com as normas de segurança;

**Ambiente de produção:** conjunto de recursos pelos quais se processam os dados de interesse da administração tributária no Ambiente Informatizado;

**Ambiente de prospecção:** conjunto de recursos utilizados para pesquisa de metodologias, técnicas, processos, tecnologias e produtos;

**Ambiente de treinamento:** conjunto de recursos utilizados para capacitar usuários frente aos sistemas e demais ativos de informação;

**Atualizar:** alterar dados de conta;

**Autoridade Certificadora(AC):** é um órgão autorizado a emitir Certificados Digitais pelo Instituto Nacional de Tecnologia da Informação (ITI), órgão do Governo Federal ligado à Presidência da República. O ITI é a primeira autoridade da cadeia de certificação, a chamada AC Raiz (Autoridade Certificadora Raiz), que emite e controla a ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileira), modelo de Certificação Digital adotado no País.

**Autoridade de Registro (AR):** faz o reconhecimento presencial da pessoa que solicita a Certificação Digital. Atualmente, são 400 AR no Brasil. A expectativa do ITI é de que até o final do ano esse número suba para 1,2 mil. Entidades como Correios, Caixa Econômica Federal, Banco do Brasil, Bradesco, Itaú, e Itaútec são AR. O ITI informou que os corretores de seguro deverão se tornar AR, o objetivo é que eles possam ir até os cidadãos para identificá-los. Ao solicitar a Certificação junto a uma AC a pessoa será orientada a procurar uma AR próxima;

**Bloquear:** inibir o acesso de uma conta a segmento do Ambiente Informatizado;

**Cadastrar:** criar identidade de usuário perante segmento do Ambiente Informatizado, associando-lhe uma conta;

**Chave privada:** número primo longo que é armazenado no cartão inteligente onde somente o usuário que tem a senha de acesso ao cartão pode acessá-la;

**Chave pública:** número primo longo que é disponibilizado a todos que querem estabelecer alguma transação com criptografia com o detentor da chave privada por da chave pública;

**Conta:** identificador de usuário, processo, serviço ou grupo de usuários utilizado pelo controle de acesso;

**Conta de serviço:** aquela necessária à execução de serviços de rede, de sistemas ou de aplicativos;

**Conta de usuário:** aquela de uso pessoal, intransferível e que identifica o usuário quando do acesso aos recursos do ambiente;

**Conta pública:** aquela utilizada para acesso a informações de domínio público.

**Convergência digital:** tendência para a transformação de todas as tecnologias em formato não digital para o formato digital, como por exemplo a transmissão de sinal televisivo que passará de analógico para digital em 2008 no Brasil.

**Coronelismo** -> prática de cunho político-social, própria do meio rural e das pequenas cidades do interior, que floresceu durante a Primeira República (1889-1930) e que configura uma forma de mandonismo em que uma elite, encarnada emblematicamente pelo proprietário rural, controla os meios de produção, detendo o poder econômico, social e político local.

**Criptografia:** técnica de transformar dados em códigos indecifráveis para serem transportados de um ponto a outro sigilosamente. A chave (pública ou privada) é o que permite decodificar estes dados.

**Desabilitar:** dissociar um perfil de uma conta;

**Desbloquear:** restaurar o acesso de uma conta a segmento do Ambiente Informatizado;

**Documento eletrônico:** também conhecido como cartão inteligente ou smartcard.

Dispositivo que armazena a chave privada do usuário;

**Equipamento de Rede e Comunicação:** conjunto de hardware e software destinado a promover o tráfego de dados no ambiente de rede local ou de longa distância;

**Equipamento Servidor:** conjunto de hardware e software que disponibiliza recursos e serviços computacionais aos usuários;

**Excluir:** eliminar uma conta;

**Habilitar:** associar um perfil a uma conta;

**Nome da Conta:** um número ou uma sequência de caracteres associados a uma conta;

**Parâmetro de normalidade:** paradigma que representa a atividade usual e legítima do usuário no acesso lógico a um sistema;

**Perfil:** conjunto de atividades atribuídas a um usuário materializado em um conjunto de privilégios ou transações;

**Princípio de segregação:** funções potencialmente conflitantes, como autorização, aprovação, execução, controle e contabilização das operações devem ser executadas por pessoas diferentes permitindo a conferência dos trabalhos evitando-se assim incorreções.

**Privilégios Administrativos:** privilégios que permitem a execução de atividades típicas de administração de um segmento do Ambiente Informatizado;

**Rede Anexada:** rede local integrante do Ambiente Informatizado da SRF instalada em local sob permissão ou concessão

**Senha de serviço:** aquela associada a uma conta de serviço ou necessária à execução de serviços de rede, de sistemas ou de aplicativos;

**Senha de setup:** aquela necessária à configuração de hardware;

**Senha de usuário:** aquela associada a uma conta de usuário, de uso pessoal e intransferível, para acesso do usuário aos recursos do ambiente;

**Senha pública:** aquela utilizada para acesso a informações de domínio público;

**Smartcard:** também conhecido como documento eletrônico. Dispositivo que gera e armazena a chave privada do usuário;

**Transação:** conjunto de operações que desempenha uma função lógica em um software;

**Usuário:** pessoa física formalmente autorizada a acessar o Ambiente Informatizado;

**Vigência:** período em que uma conta, transação, conjunto de privilégios de acesso ou relacionamentos entre esses elementos podem ser usados;

## Apêndice A – Questionário utilizado

Questionário destinado aos Gestores de Segurança da Informação da 7ª RF da RFB

1. Para se resolver o problema das diversas contas de usuário, múltiplas senhas e obrigatoriedade de constantes mudanças de palavras secretas, quase que obrigando o usuário a fazer anotações, você acredita que a utilização do *smartcard* ou cartão inteligente (Certificado Digital) solucionaria a questão, não prejudicando a disponibilidade, integridade e disponibilidade (CID) dos sistemas, garantindo a irretrabilidade dentro da legalidade? Justifique a sua resposta!
2. Em caso negativo, qual seria a solução na sua opinião?
3. Em caso afirmativo, você faria a sugestão de utilização de alguma outra tecnologia para auxiliar a utilização do Certificado Digital?

## **Apêndice B - SPED**

### **DECRETO Nº 6.022, DE 22 DE JANEIRO DE 2007.**

Institui o Sistema Público de Escrituração Digital - Sped

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso IV, da Constituição, e considerando o disposto no art. 37, inciso XXII, da Constituição, nos arts. 10 e 11 da Medida Provisória no 2.200-2, de 24 de agosto de 2001, e nos arts. 219, 1.179 e 1.180 da Lei no 10.406, de 10 de janeiro de 2002,

DECRETA:

Art. 1º Fica instituído o Sistema Público de Escrituração Digital - Sped.

Art. 2º O Sped é instrumento que unifica as atividades de recepção, validação, armazenamento e autenticação de livros e documentos que integram a escrituração comercial e fiscal dos empresários e das sociedades empresárias, mediante fluxo único, computadorizado, de informações.

§ 1º Os livros e documentos de que trata o caput serão emitidos em forma eletrônica, observado o disposto na Medida Provisória no 2.200-2, de 24 de agosto de 2001.

§ 2º O disposto no caput não dispensa o empresário e a sociedade empresária de manter sob sua guarda e responsabilidade os livros e documentos na forma e prazos previstos na legislação aplicável.

Art. 3º São usuários do Sped:

I - a Secretaria da Receita Federal do Ministério da Fazenda;

II - as administrações tributárias dos Estados, do Distrito Federal e dos Municípios, mediante convênio celebrado com a Secretaria da Receita Federal; e

III - os órgãos e as entidades da administração pública federal direta e indireta que tenham atribuição legal de regulação, normatização, controle e fiscalização dos empresários e das sociedades empresárias.

§ 1º Os usuários de que trata o caput, no âmbito de suas respectivas competências, deverão estabelecer a obrigatoriedade, periodicidade e prazos de apresentação dos livros e documentos, por eles exigidos, por intermédio do Sped.

§ 2o Os atos administrativos expedidos em observância ao disposto no § 1º deverão ser implementados no Sped concomitantemente com a entrada em vigor desses atos.

§ 3o O disposto no § 1o não exclui a competência dos usuários ali mencionados de exigir, a qualquer tempo, informações adicionais necessárias ao desempenho de suas atribuições.

Art. 4o O acesso às informações armazenadas no Sped deverá ser compartilhado com seus usuários, no limite de suas respectivas competências e sem prejuízo da observância à legislação referente aos sigilos comercial, fiscal e bancário.

Parágrafo único. O acesso previsto no caput também será possível aos empresários e às sociedades empresárias em relação às informações por eles transmitidas ao Sped.

Art. 5o O Sped será administrado pela Secretaria da Receita Federal com a participação de representantes indicados pelos usuários de que tratam os incisos II e III do art. 3o.

§ 1o Os usuários do Sped, com vistas a atender o disposto no § 2o do art. 3o, e previamente à edição de seus atos administrativos, deverão articular-se com a Secretaria da Receita Federal por intermédio de seu representante.

§ 2o A Secretaria da Receita Federal, sempre que necessário, poderá solicitar a participação de representantes dos empresários e das sociedades empresárias, bem assim de entidades de âmbito nacional representativas dos profissionais da área contábil, nas atividades relacionadas ao Sped.

Art. 6o Compete à Secretaria da Receita Federal:

I - adotar as medidas necessárias para viabilizar a implantação e o funcionamento do Sped;

II - coordenar as atividades relacionadas ao Sped;

III - compatibilizar as necessidades dos usuários do Sped; e

IV - estabelecer a política de segurança e de acesso às informações armazenadas no Sped, observado o disposto no art. 4o.

Art. 7o O Sped manterá, ainda, funcionalidades de uso exclusivo dos órgãos de registro para as atividades de autenticação de livros mercantis.

Art. 8o A Secretaria da Receita Federal e os órgãos a que se refere o inciso III do art. 3o expedirão, em suas respectivas áreas de atuação, normas complementares ao cumprimento do disposto neste Decreto.

§ 1o As normas de que trata o caput relacionadas a leiautes e prazos de apresentação de informações contábeis serão editadas após consulta e, quando couber, anuência dos usuários do Sped.

§ 2o Em relação às informações de natureza fiscal de interesse comum, os leiautes e prazos de apresentação serão estabelecidos mediante convênio celebrado entre a Secretaria da Receita Federal e os usuários de que trata o inciso II do art. 3º.

Art. 9o Este Decreto entra em vigor na data de sua publicação.

Brasília, 22 de janeiro de 2007; 186º da Independência e 119º da República.

LUIZ INÁCIO LULA DA SILVA

Bernard Appy

## **Apêndice B – Política de segurança da adm. federal**

### **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 2.190, 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 criptográficos, 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 emanções 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.

§ 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.

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 D.O. de 14.6.2000*

## **Apêndice C – Certificação digital na adm. federal**

### **DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001.**

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

**O VICE-PRESIDENTE DA REPÚBLICA**, no exercício do cargo de Presidente da República, usando das atribuições que lhe confere o art. 84, incisos II, IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

#### **DECRETA:**

Art. 1º A prestação de serviços de certificação digital no âmbito da Administração Pública Federal, direta e indireta, fica regulada por este Decreto.

Art. 2º Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital.

§ 1º Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

§ 2º Respeitado o disposto no § 1º, o Comitê Executivo do Governo Eletrônico poderá estabelecer padrões e requisitos administrativos para a instalação de Autoridades Certificadoras - AC e de Autoridades de Registro – AR próprias na esfera da Administração Pública Federal.

§ 3º As AR de que trata o § 2º serão, preferencialmente, os órgãos integrantes do Sistema de Administração do Pessoal Civil - SIPEC.

Art. 3º A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil.

Art. 3º-A. As aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil. (Incluído pelo Decreto nº 4.414, de 7.10.2002)

Art. 4º Será atribuída, na Administração Pública Federal, aos diferentes tipos de certificados disponibilizados pela ICP-Brasil, a classificação de informações segundo o estabelecido na legislação específica.

Art. 5º Este Decreto entra em vigor na data de sua publicação.

Art. 6º Fica revogado o Decreto nº 3.587, de 5 de setembro de 2000.  
Brasília, 31 de outubro de 2001; 180º da Independência e 113º da República.

MARCO ANTONIO DE OLIVEIRA MACIEL

*Martus Tavares*

*Silvano Gianni*

## Apêndice D – Criptografia

Fonte: <http://www.infowester.com/criptografia.php> em 30/08/2007

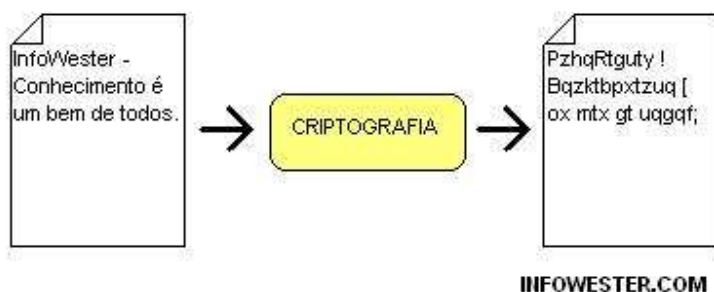
### Introdução

O envio e o recebimento de informações sigilosas é uma necessidade antiga, que existe há centenas de anos. Com o surgimento da internet e sua facilidade de entregar informações de maneira precisa e extremamente rápida, a criptografia tornou-se uma ferramenta fundamental para permitir que apenas o emissor e o receptor tenham acesso livre à informação trabalhada. Este artigo tem por objetivo dar uma abordagem introdutória à criptografia, mostrando os aspectos e conceitos mais importantes.

### O que é Criptografia

O termo Criptografia surgiu da fusão das palavras gregas "Kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la. Para isso, uma série de técnicas são usadas e muitas outras surgem com o passar do tempo.

Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas "chaves criptográficas". Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação.



Os primeiros métodos criptográficos existentes usavam apenas um algoritmo de codificação. Assim, bastava que o receptor da informação conhecesse esse algoritmo para poder extraí-la. No entanto, se um intruso tiver posse desse algoritmo, também poderá decifrá-la, caso capture os dados criptografados. Há ainda outro problema: imagine que a pessoa A tenha que enviar uma informação criptografada à pessoa B. Esta última terá que conhecer o algoritmo usado. Imagine agora que uma pessoa C também precisa receber uma informação da pessoa A, porém a pessoa C não pode descobrir qual é a informação que a pessoa B recebeu. Se a pessoa C capturar a informação enviada à pessoa B, também conseguirá decifrá-la, pois quando a pessoa A enviou sua informação, a pessoa C também teve que conhecer o algoritmo usado. Para a pessoa A evitar esse problema, a única solução é usar um algoritmo diferente para cada receptor.

Com o uso de chaves, um emissor pode usar o mesmo algoritmo (o mesmo método) para vários receptores. Basta que cada um receba uma chave diferente. Além disso, caso um receptor perca ou exponha determinada chave, é possível trocá-la, mantendo-se o mesmo algoritmo.

Você já deve ter ouvido falar de chave de 64 bits, chave de 128 bits e assim por diante. Esses valores expressam o tamanho de uma determinada chave. Quanto mais bits forem utilizados, mais segura será a criptografia. Explica-se: caso um algoritmo use chaves de 8 bits, apenas 256 chaves poderão ser usadas na decodificação, pois 2 elevado a 8 é 256. Isso deixa claro que 8 bits é inseguro, pois até uma pessoa é capaz de gerar as 256 combinações (embora demore), imagine então um computador. Porém, se forem usados 128 ou mais bits para chaves, haverá uma quantidade extremamente grande de combinações, deixando a informação criptografada bem mais segura.

### **Chaves simétricas e assimétricas**

Existem dois tipos de chaves: simétricas e assimétricas. Ambas são vistas a seguir.

#### **Chave simétrica**

Esse é um tipo de chave mais simples, onde o emissor e o receptor fazem uso da mesma chave, isto é, uma única chave é usada na codificação e na decodificação da informação. Existem vários algoritmos que usam chaves simétricas, como o DES, o IDEA, e o RC:

**DES (Data Encryption Standard):** criado pela IBM em 1977, faz uso de chaves de 56 bits. Isso corresponde a 72 quadrilhões de combinações. É um valor absurdamente alto, mas não para um computador potente. Em 1997, ele foi quebrado por técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet;

**IDEA (International Data Encryption Algorithm):** criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES. Sua implementação em software é mais fácil do que a implementação deste último;

**RC (Ron's Code ou Rivest Cipher):** criado por Ron Rivest na empresa RSA Data Security, esse algoritmo é muito utilizado em e-mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões: RC2, RC4, RC5 e RC6. Essencialmente, cada versão difere da outra por trabalhar com chaves maiores.

Há ainda outros algoritmos conhecidos, como o AES (Advanced Encryption Standard) - que é baseado no DES - , o 3DES, o Twofish e sua variante Blowfish, entre outros.

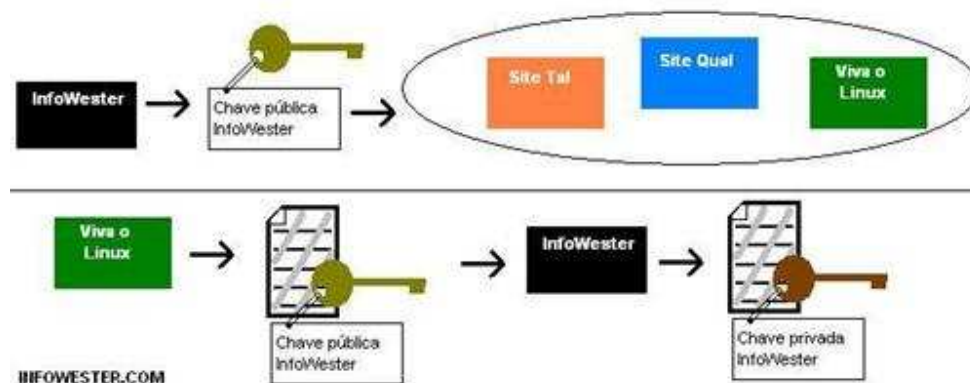
O uso de chaves simétricas tem algumas desvantagens, fazendo com que sua utilização não seja adequada em situações onde a informação é muito valiosa. Para começar, é necessário usar uma grande quantidade de chaves caso muitas pessoas estejam envolvidas. Ainda, há o fato de que tanto o emissor quanto o receptor precisa conhecer a chave usada. A transmissão dessa chave de um para o outro pode não ser tão segura e cair em "mãos erradas".

### **Chave assimétrica**

Também conhecida como "chave pública", a chave assimétrica trabalha com duas chaves: uma denominada privada e outra denominada pública. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta - a chave privada - é secreta.

Para entender melhor, imagine o seguinte: O InfoWester criou uma chave pública e a enviou a vários outros *sites*. Quando qualquer desses *sites* quiser enviar uma informação criptografada ao InfoWester deverá utilizar a chave pública deste. Quando o InfoWester receber a informação, apenas será possível extraí-la com o uso da chave privada, que só o

InfoWester tem. Caso o InfoWester queira enviar uma informação criptografada a outro *site*, por exemplo, o Viva o Linux, deverá conhecer sua chave pública.



Entre os algoritmos que usam chaves assimétricas, têm-se o RSA (o mais conhecido) e o Diffie-Hellman:

**RSA (Rivest, Shamir and Adleman):** criado em 1977 por Ron Rivest, Adi Shamir e Len Adleman nos laboratórios do MIT (Massachusetts Institute of Technology), é um dos algoritmos de chave assimétrica mais usados. Nesse algoritmo, números primos (número primo é aquele que só pode ser dividido por 1 e por ele mesmo) são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor. Porém, descobrir os dois primeiros números a partir do terceiro (ou seja, fazer uma fatoração) é muito trabalhoso. Se dois números primos grandes (realmente grandes) forem usados na multiplicação, será necessário usar muito processamento para descobri-los, tornando essa tarefa quase sempre inviável. Basicamente, a chave privada no RSA são os números multiplicados e a chave pública é o valor obtido;

**ElGamal:** criado por Taher ElGamal, esse algoritmo faz uso de um problema matemático conhecido por "logaritmo discreto" para se tornar seguro. Sua utilização é freqüente em assinaturas digitais.

Existem ainda outros algoritmos, como o DSA (Digital Signature Algorithm), o Schnorr (praticamente usado apenas em assinaturas digitais) e Diffie-Hellman.

## PGP

PGP é a sigla para Pretty Good Privacy. Trata-se de um software livre de criptografia criado por Philip Zimmermman em 1991. A intenção de Zimmermman foi a de ajudar na defesa da liberdade individual nos Estados Unidos e no mundo inteiro, uma vez que ele percebeu que o uso do computador seria algo cada vez mais maior e que o direito à

privacidade deveria ser mantido nesse meio. Por ser disponibilizado de forma gratuita, o PGP acabou se tornando um dos meios de criptografia mais conhecidos, principalmente na troca de e-mails.

No PGP, chaves assimétricas são usadas. Além disso, para reforçar a segurança, o software pode realizar um segundo tipo de criptografia através de um método conhecido como "chave de sessão" que, na verdade, é um tipo de chave simétrica.

Um fato curioso a ser citado é que Zimmermann foi alvo de uma investigação policial que durou quase 3 anos. Isso porque a legislação americana proíbe a exportação de software criptográfico sem expressa autorização do governo. Porém, na investigação, ficou provado que alguém sem identificação e não o próprio Zimmermann é que distribuiu o programa pela internet. O PGP então passou a ser enviado para outros países através de uma brecha na legislação americana: novas versões tiveram seu código-fonte publicado em livros. Estes são exportados de forma legal, pois a lei americana proíbe a exportação do software, mas o código impresso não é considerado programa.

Existem vários softwares baseados no PGP. Para mais informações e downloads (inclusive do código-fonte) visite [www.pgp.com](http://www.pgp.com).

### **Finalizando**

Criptografia só pode ser considerada como tal se 4 princípios básicos forem seguidos e oferecidos: confidencialidade, autenticação, integridade da informação e não repudiabilidade (o remetente não pode negar o envio da informação). É por isso que a criptografia é um recurso tão importante na transmissão de informações pela internet e, mesmo assim, não é capaz de garantir 100% de segurança, pois sempre existe alguém que consegue criar um jeito de quebrar uma codificação. Por isso é que técnicas existentes são aperfeiçoadas e outras são criadas, como a "Criptografia Quântica". Na criptografia há ainda outros conceitos envolvidos, como a Função Hashing (usada em assinaturas digitais), e aplicações, como a Certificação Digital.

Para quem deseja trabalhar com computação, criptografia é uma área interessante. Obviamente, é necessário ter muita afinidade com cálculos, afinal, como pode ser notado no artigo, matemática é a base para os conceitos que envolvem a criptografia.

Escrito por Emerson Alecrim - Publicado em 12/08/2005 - Atualizado em 12/08/2005.