Segurança da Informação

Helena C. De S. Sacerdote Costa
helenacs@tba.com.br

Sumário

1. *Introdução* 3
2. *Conceitos* 5
3. *Ameaças a Segurança de Informação* 8
4. *Definição de Política de Segurança* 9
5. *Princípios de Segurança da Informação* 10
6. *Política de Segurança da Informação no Brasil* 11
7. *Lei da Assinatura Digital nos EUA – e-Sign Bill* 12
8. *Conclusão* 13
9. *Anexos* 14
10. *Fontes de Referências* 19

1. Introdução

Axioma da segurança:
"Uma corrente não é mais forte do que o seu elo mais fraco".

Durante as primeiras décadas de sua existência, as redes de computadores foram principalmente usadas por pesquisadores universitários, para enviar mensagens de correio eletrônico e por funcionários de empresas, para compartilhar impressoras. Sob essas condições, a segurança nunca precisou de maiores cuidados. Mas atualmente, como milhões de cidadãos comuns estão usando as redes para executar operações bancárias, fazer compras e declarar seus impostos, a segurança das redes está despontando no horizonte como um problema em potencial.

A segurança é um assunto abrangente e inclui inúmeros tipos de pecados. Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou modifiquem mensagens enviadas a outros destinatários. Outra preocupação da segurança se volta para as pessoas que tentam ter acesso a serviços remotos, os quais elas não estão autorizadas a usar. Ela também permite que se faça a distinção entre uma mensagem supostamente verdadeira e um trote. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas, além de lidar com pessoas que negam terem enviado determinadas mensagens.

A maior parte dos problemas de segurança são intencionalmente causadas por pessoas que tentam obter algum benefício ou prejudicar alguém.

São medidas para garantir a segurança adequada em uma organização:

- avaliar os riscos;
  Deve-se perguntar:
  - Proteger O QUE?
  - Proteger DE QUEM?
  - Proteger A QUE CUSTOS?
  - Proteger COM QUE RISCOS?

- rever a política de segurança para atender a quaisquer mudanças nos níveis de risco;
- implementar os controles de segurança que atendam aos requisitos da política;
- monitorar e manter a eficácia dos controles de segurança.

No âmbito do Governo Federal, a questão da segurança da informação está recebendo um tratamento destacado e permanente, com a "Política de Segurança da Informação nos Órgãos do Poder Executivo Federal – PSIPE", conforme o Decreto n.º 3.505, de 13 de junho de 2000.

As autoridades governamentais estão trabalhando no sentido de aprovar leis sobre crimes na Internet; leis para crimes contra a Previdência Social (o que tipifica o crime eletrônico); leis que prevêem a obrigatoriedade da assinatura digital e a existência de uma fatura eletrônica nas operações financeiras on-line, para garantir a segurança e a privacidade das transações de negócios pela Internet.

Embora medidas sejam tomadas no intuito de promover segurança da informação, a questão será sempre muito mais complexa do que parece. Quase todas as pessoas acham que o uso de um sistema simples qualquer, bastará para garantir a sua segurança. Até empresas renomadas não têm sido eficazes no que diz respeito a segurança que oferecem aos usuários dos seus produtos.

Um bom exemplo disso é o sistema de criptografia de um editor de texto famoso de uma companhia que domina o mercado. O sistema é tão fraco que há programas livremente circulando na Internet que o quebram em segundos. Isto significa que os planejadores e programadores do sistema de criptografia deste editor de textos não se informaram adequadamente sobre esta ciência. Além disto pode-se dizer que falhas como esta são muito graves, pois põem em risco a integridade do usuário que inocentemente é levado a crer que o sistema é seguro.

2. Conceitos

- **Assinatura Digital**: método baseado na criptografia assimétrica visando garantir que determinada mensagem não seja alterada durante seu trajeto. Quando se utiliza um aplicativo para assinar digitalmente uma mensagem, basicamente é anexado a parte pública do Certificado Digital à mensagem, juntamente com outras informações que garantem a integridade do e-mail. Antes da mensagem de e-mail e o Certificado Digital serem enviados, a mensagem passa por um processo de codificação chamado *algoritmo hash*, através do qual a mensagem que está sendo enviada é utilizada para gerar matematicamente um conjunto de caracteres (letras e números), que só poderiam ser criados especificamente pela mensagem. Esse conjunto leva o nome de *message digest* (resumo da mensagem). Se assinar um documento, não se pode renegar a assinatura, alegando que foi falsificada. (*não-repúdio*)

- **Algoritmo Hash**: equação matemática que utiliza texto (tal como uma mensagem de e-mail) para criar um código chamado message digest (resumo de mensagem).

- **Autenticação**: Quando uma entidade precisa provar para outra a sua identidade.

- **Autoridade Certificadora (CA)**: Quando sua companhia emite um Certificado Digital, ela está lhe fornecendo um meio se identificar às outras pessoas e aos sócios da companhia ou aos computadores da rede.

- **Certificado Digital**: utilizam a tecnologia conhecida como criptografia de chave pública. Na fase inicial de inscrição para o Certificado Digital, o computador cria duas chaves: a pública, que vem com seu certificado e está afixada no repositório da Autoridade Certificadora (CA), e a privativa, que fica no computador. A CA não tem acesso a sua chave privativa. Geralmente fica no computador e nunca é transmitida para a CA. A integridade do certificado ("identidade digital") depende da chave privativa ser controlada exclusivamente pelo usuário.
- **Chave Privativa**: Chave matemática (mantida em segredo pelo usuário) usada para criar assinaturas digitais e, dependendo do algoritmo, para decriptografar mensagens ou arquivos criptografados com a chave pública correspondente.

- **Chave Pública**: Chave matemática que pode ser compartilhada com segurança, de modo que outros possam lhe enviar informações criptografadas, e que somente sua chave privativa pode decodificar. A chave pública pode também confirmar a veracidade de assinaturas criadas com suas chaves privativas correspondentes. Dependendo do algoritmo, as chaves públicas também podem ser utilizadas para criptografar arquivos ou mensagens que são decriptografados com as chaves privativas correspondentes.

- **Criptografia**: tão antiga quanto a própria escrita, consiste na ciência e na arte de se comunicar secretamente. Tem por objetivo básico tornar uma mensagem ininteligível para um adversário, que possa vir a interceptá-la. Historicamente, quatro grupos de pessoas utilizaram e contribuíram para a arte da criptografia: os militares, os diplomatas, as pessoas que gostam de guardar memórias e os amantes. Dentre eles, os militares tiveram o papel mais importante e definiram as bases para a tecnologia. Dentro das organizações militares, tradicionalmente as mensagens a serem cifradas eram entregues a auxiliares que se encarregam de criptografá-las e transmiti-las. O grande volume de mensagens impedia que esse trabalho fosse feito por poucos especialistas. Até o advento dos computadores, uma das principais restrições da criptografia era a habilidade do auxiliar de criptografia fazer as transformações necessárias, em geral com poucos equipamentos e no campo de batalha. Uma outra restrição era a dificuldade de alternar os métodos criptográficos rapidamente, pois isso exigia a repetição do treinamento de um grande número de pessoas. No entanto, o perigo de um auxiliar de criptografia ser capturado pelo inimigo tornou indispensável a possibilidade de alterar o método criptográfico instantaneamente, se necessário. A arte de criar mensagens cifradas (criptografia) e solucioná-las (criptoanálise) é coletivamente chamada de criptologia (criptology).

- **Criptografia assimétrica:** as mensagens a serem criptografadas, conhecidas como texto simples, são transformadas por uma função que é parametrizada por um par de chaves: uma chave privativa e uma pública. A chave privativa é única e fica na máquina do usuário, protegida por senha. A chave pública é distribuída pelo usuário a todos que ele desejar. Com ela, as outras pessoas podem criptografar as mensagens enviadas para aquele usuário. Em seguida, a saída do processo de criptografia, é conhecida como texto cifrado.

- **Inimigo**: adversário ou oponente do remetente ou do destinatário da informação, não sendo necessariamente alguém com motivos torpes. um

exemplo disso pode ser a polícia querendo fazer a análise criptográfica dos dados criptografados armazenados no computador de um criminoso.

- **Inimigo ativo**: é aquele que intercepta a mensagem e tenta interferir no processo de comunicação. Mesmo que não esteja interessado em decriptar a mensagem interceptada, pode adulterá-la ou utilizá-la para obter algo.

- **Inimigo passivo**: é aquele que intercepta a mensagem e tenta ganhar conhecimentos através dela, mas não interfere no processo de comunicação. Normalmente age como espião que tenta roubar informações.

- **Message Digest**: representa uma mensagem ou documento de maior extensão. É como a "impressão digital" de um documento maior. É usado para criar uma assinatura digital que será exclusiva de um determinado documento. Um message digest não revela o conteúdo de um documento. Isto é, mesmo que se consiga visualizá-lo, não será possível imaginar o que a mensagem original contém. MD2, MD4 e MD5 (MD significa Message Digest) são funções hash amplamente utilizadas, destinadas especificamente ao uso criptográfico. Elas geram digests de 128 bits e não se tem conhecimento de nenhum ataque mais rápido do que a busca exaustiva.

- **Não–repúdio**: Previne tanto o emissor contra o receptor, quanto previne contra a negação de uma mensagem transmitida.

- **Par de chaves**: consiste na *chave privativa* e na *chave pública* correspondente. A chave privativa geralmente é protegida por uma senha e armazenada no computador. Só é conhecida pelo portador e não é enviada a ninguém. A chave pública é compartilhada com outras pessoas, outros computadores e outros sites da Web.

- **Segurança da informação**[1]: 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 ameaça a seu desenvolvimento.

[1] Conceituação segundo o DOU de 14/06/2000 - Decreto 3.505 de 13/06/2000.

3. Ameaças a Segurança de Informação

Ameaças de *inimigo ativo*:

- Interrupção: a mensagem enviada não chega ao destinatário e o inimigo pode ou não interceptar a mensagem;
- Modificação: o inimigo intercepta a mensagem e a substitui por outra elaborada por ele;
- Fabricação: o inimigo gera mensagens falsas para o destinatário e as insere no canal.

Objetivos do *inimigo ativo*:

- Personificação (disfarce): o inimigo quer se fazer passar por uma outra pessoa, falsificando mensagens ou tentando conseguir acesso a um sistema;
- Repetição: o inimigo possui uma mensagem previamente interceptada e tenta usá-la novamente;
- Modificação: o inimigo intercepta a mensagem e a substitui por outra elaborada por ele;
- Negação de serviço: o inimigo atrapalha o funcionamento do sistema.

Casos clássicos de invasão eletrônica:

Verme (worm) na Internet Um aluno de graduação da Universidade de Cornell, Robert Morris Jr., paralisou cerca de 3.000 computadores conectados à Internet em 02 de novembro de 1988 (cerca de 50% da Internet na época). Embora o verme não tivesse efeitos destrutivos, a rede só conseguiu voltar ao normal alguns dias depois. O estudante foi sentenciado, em 1990, a 3 anos de prisão, mais multa de U$ 10.000,00, mais 400 horas de serviço comunitário.

Conexão KGB Em 1988, um espião da Alemanha Oriental tentou violar 450 computadores na área acadêmica e militar; vendia as informações para a KGB.

Caso Kevin Mitnick Causou danos à DEC, com o roubo de um sistema de segurança secreto; roubou cerca de 20.000 números de cartão de crédito; atacou o computador de um especialista de segurança em informática; perseguido pelo FBI, foi preso em 1995, e pode pegar até 20 anos de prisão, além de multa de U$ 500.000,00.

4. Definição de Política de Segurança

Política de segurança da informação é uma declaração ampla dos objetivos e intenções da organização com relação à conexão e ao uso. Normalmente, ela deve especificar o seguinte:

- os serviços que podem ser usados;
- quem autoriza as conexões;
- quem é responsável pela segurança;
- as normas, diretrizes e práticas a serem obedecidas;
- as responsabilidades dos usuários.

Uma questão fundamental é decidir quem será responsável pela segurança na organização. Todos os usuários terão um papel a desempenhar, mas, em última análise, os gerentes de alto escalão são os responsáveis por assegurar a implementação e manutenção dos controles de segurança adequados.

Isto é necessário para assegurar que as informações e os ativos da organização estarão protegidos contra um ataque através do serviço oferecido na Internet.

5. Princípios de Segurança da Informação[2]

- Disponibilidade: Considera-se este princípio quando um sistema, ou ativo de informação precisa estar disponível para satisfazer os seus requisitos ou evitar perdas financeiras.
- Integridade: Considera-se este princípio quando um sistema, ou ativo de informação, contém informação que deve ser protegida contra modificações não autorizadas, imprevistas ou até mesmo não intencionais, incluindo ainda mecanismos que permitam a detecção de tais tipos de alteração.
- Confidencialidade: Considera-se este princípio quando um sistema, ou ativo de informação, necessita de proteção contra a divulgação não autorizada dos seus bens de informação.
- Autenticidade: Considera-se este princípio para atestar, com exatidão, o originador do dado ou informação, e permitir o não-repúdio quanto a transmissão ou recepção do mesmo.

[2] Princípios extraídos de recomendações da OCDE - organização para Cooperação e Desenvolvimento Econômico

6. Política de Segurança da Informação no Brasil

Existe uma grande preocupação do Governo Federal em assegurar a proteção da informação do governo e dos cidadãos. É fundamental garantir o direito dos cidadãos à privacidade, além do direito à consulta sobre os dados coletados nos sistemas governamentais, previsto na Constituição. Os websites públicos devem comprometer-se a garantir a confidencialidade das informações de caráter pessoal que são armazenadas em suas bases de dados, sejam elas relativas aos usuários ou pessoas que compõem a administração pública.

Conforme abordado na Introdução, a questão da segurança da informação está recebendo atenção do Governo Federal, que sancionou o Decreto que institui a "Política de Segurança da Informação nos Órgãos do Poder Executivo Federal – PSIPE", conforme o Decreto n.º 3.505, de 13 de junho de 2000.

Caberá à Secretaria-Executiva do Conselho de Defesa Nacional - SECDN, órgão vinculado ao Gabinete de Segurança Institucional da Presidência da República, assessorada pelo Comitê Gestor da Segurança da Informação - CGSI propor as diretrizes para implementação da Política no âmbito do Poder Executivo Federal.

O Governo Federal desenvolverá a PSIPE de acordo com as diretrizes do Comitê e contará com o apoio técnico/operacional da Câmara Técnica de Segurança da Tecnologia da Informação Œ CT-STI/SISP. Por sua vez, a Secretaria de Logística e Tecnologia da Informação - SLTI do Ministério do Planejamento, Orçamento e Gestão exercerá um papel preponderante na implementação da PSIPE, pois tem entre suas atribuições a competência de coordenar as atividades do Sistema de Administração de Recursos de Informação e Informática - SISP, propondo políticas, diretrizes e normas de Informação e Informática, no âmbito da Administração Pública Federal direta, autárquica e fundacional.

7. Lei da Assinatura Digital nos EUA – e-Sign Bill

No mês de julho deste ano, o presidente dos Estados Unidos Bill Clinton, sancionou a lei oficialmente conhecida como Lei da Assinatura Digital, ou Eletronic Signatures in Global and National Commerce Act- simplificada para e-Sign Bill. A lei dará às assinaturas eletrônicas o mesmo poder legal conferido às elaboradas com tintas sobre o papel. Ela elimina as barreiras legais no uso de tecnologia eletrônica para elaborar e assinar contratos, reunir e armazenar documentos. A legislação permitirá que consumidores e comerciantes assinem cheques, preencham solicitações de empréstimo ou de serviços, sem a necessidade de uma assinatura em papel.

A legislação sobre a assinatura digital, aprovada na Câmara e no Senado por ampla margem no início de junho, é considerada como o início de uma era de comércio eletrônico na qual as empresas poderão realizar transações completas on-line, em vez de comparecer pessoalmente.

A medida estipula que os consumidores devem concordar em realizar negócios on-line terão as proteções de consumidor equivalentes àquelas existentes no mundo do papel. Segundo a legislação, nenhum contrato, assinatura ou registro poderá ter seu efeito legal negado por estar somente em formato eletrônico.

A *e-Sign Bill* não se compromete com nenhuma solução tecnológica já disponível. Pessoas e empresas poderão escolher livremente o provedor do serviço responsável pela veracidade das assinaturas digitais. Ferramentas de autenticação eletrônica já existentes ganharão mercado a partir da legalização dos certificados digitais.

8. Conclusão

A criptografia tenta garantir a segurança eletrônica, mas a maior parte das falhas de sistemas criptográficos não são devido a erros ou falhas nos algoritmos, mas sim a erros ou falhas humanas. Uma empresa especializada em Segurança (Módulo) fez uma pesquisa em 350 companhias brasileiras e constatou que 19% dos ataques são provocados por funcionários.

Uma organização que busca a segurança de suas informações deve implantar um plano baseado em três pilares: difusão da cultura de segurança, ferramentas para garantir a execução do projeto e mecanismo de monitoração.

Há de se descobrir os pontos vulneráveis, avaliar os riscos, tomar as providências adequadas e investir o necessário para se ter uma segurança homogênea e suficiente.

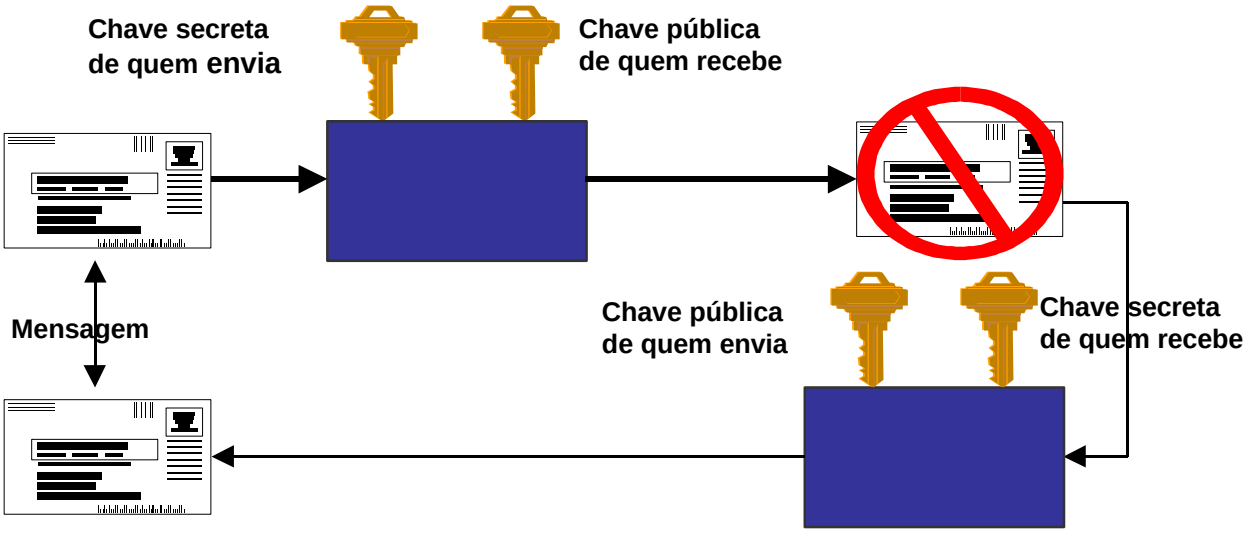
Sempre existirão riscos. O que não se pode admitir é o descaso com a segurança.

" É fácil ter-se um sistema de computação seguro.
Você meramente tem que desconectar o seu
sistema de qualquer rede externa, e permitir
somente terminais ligados diretamente a ele. Pôr
a máquina e seus terminais em uma sala fechada,
e um guarda na porta."

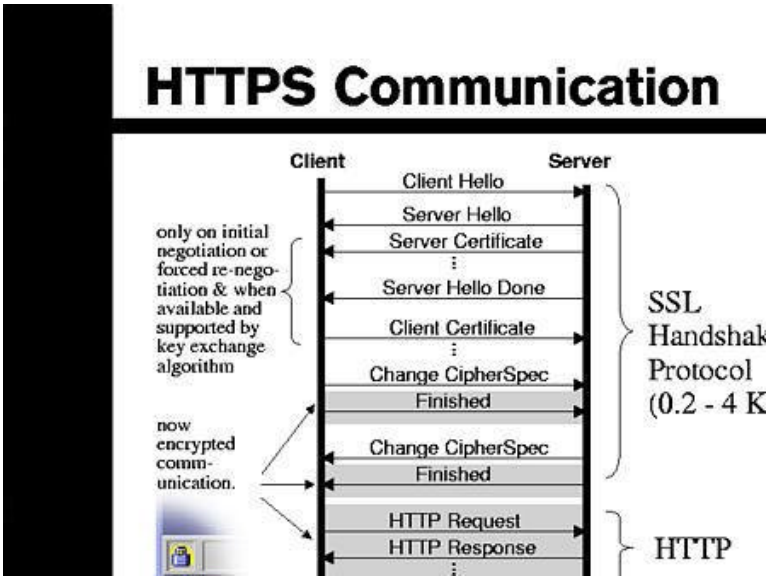
F.T. Grampp e R.H. Morris

9. Anexos

9.1.Criptografia



9.2.SSL: Encriptação de informações em rede



PGP: http://www.ifi.uio.no/pgp

9.3.Política de Segurança da Informação

DECRETO No 3.505, DE 13 DE JUNHO DE 2000.

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

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

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

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

II - proteção de assuntos que mereçam tratamento especial;

III - capacitação dos segmentos das tecnologias sensíveis;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I - Ministério da Justiça;
II - Ministério da Defesa;
III - Ministério das Relações Exteriores;
IV - Ministério da Fazenda;
V - Ministério da Previdência e Assistência Social;
VI - Ministério da Saúde;
VII - Ministério do Desenvolvimento, Indústria e Comércio Exterior;
VIII - Ministério do Planejamento, Orçamento e Gestão;
IX - Ministério das Comunicações;
X - Ministério da Ciência e Tecnologia;
XI - Casa Civil da Presidência da República; e
XII - Gabinete de Segurança Institucional da Presidência da República, que o coordenará.

§ 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

10. Fontes de Referências

10.1. Referências Bibliográficas

CARVALHO, Daniel B. **Segurança de Dados com Criptografia**. Rio de Janeiro: Book Express, 2000.
Diário Oficial da União de 14.06.2000 - Decreto No 3.505, de 13.06.2000.
Jornal **O Estado de São Paulo** de 28/06/2000
Revista **Valor Econômico** de 03/07/2000
Cartilha do Ministério do Planejamento **– A Segurança das Informações e a Internet**
Cartilha do Ministério do Planejamento **– Fundamentos do Modelo de Segurança da Informação**

10.2. Referências WWW

http://www.certisign.com.br
http://www.ifi.uio.no/pgp
http://www.redegoverno.gov.br
http://www.trueaccess.com.br/