



**Faculdade de Tecnologia de Americana**
**Curso de Processamento de dados**

# SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DA INTERNET COM ÊNFASE EM CERTIFICAÇÃO DIGITAL

**MÁRIO CÉSAR REATO BERNARDINELLI**

**Americana, SP**
**2010**



**Faculdade de Tecnologia de Americana**
**Curso de Processamento de dados**

# SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DA INTERNET COM ÊNFASE EM CERTIFICAÇÃO DIGITAL

**MÁRIO CÉSAR REATO BERNARDINELLI**

**mariocrb@yahoo.com.br**

**Monografia elaborada em cumprimento à exigência curricular do Curso de Processamento de Dados da Fatec Americana sob a orientação do Prof. Nelson Gonçalves Junior.**

**Área: Redes e Segurança da Informação**

**Americana, SP**
**2010**

**BANCA EXAMINADORA**

**Prof. Irineu Ambrozano Filho (Presidente)**

**Prof. Nelson Gonçalves Junior (Orientador)**

**Prof. Antonio Alfredo Lacerda (Convidado)**

## AGRADECIMENTOS

Gostaria, primeiramente, de agradecer a Deus, pois ele sempre permaneceu junto de mim, me fortalecendo e encorajando na realização desta monografia.

Sou grato a Faculdade de Tecnologia de Americana, que tem oferecido as ferramentas e o suporte necessário para execução desta monografia, aos professores desta instituição, dentre eles principalmente o Prof. Nelson Gonçalves Junior que me orientou e coordenou com grande eficácia.

Gostaria de agradecer também ao meu pai Antonio Tadeu Bernardinelli e a minha mãe Maria Alice Reato Bernardinelli pela paciência e apoio nos dias difíceis, ao meu tio Mario Luiz Bernardinelli que auxiliou no desenvolvimento desta e a minha noiva Vanessa Aparecida Palmiro por sua presteza e colaboração.

Enfim, a todos que colaboraram direta e indiretamente para a realização desta monografia, meus sinceros agradecimentos.

## DEDICATÓRIA

Dedico este trabalho principalmente a Deus, por ter me dado saúde, motivação e esta oportunidade de aprofundar meus conhecimentos. Aos meus pais que sempre estiveram comigo nos momentos difíceis e foram o alicerce que sempre me sustentou.

## RESUMO

A tecnologia da informação vem passando por um processo de evolução muito rápido e torna a vida de seus adeptos e usuários cada vez mais acessível, interativa, funcional e com possibilidades ilimitadas através principalmente das redes de computadores que estão distribuídas por todo o mundo, na qual, a internet vem alavancando esse processo, porém, com ela a necessidade de garantir a segurança da informação com intuito de salvaguardar e manter o sigilo de informações confidenciais ou até mesmo identificar computadores, pessoas e diversos dispositivos, para então, disponibilizar acesso a estes de conteúdos e serviços diferenciados e restritos. A Certificação digital é uma solução para o problema de segurança da informação em redes públicas e privadas, no qual, permite uma maior garantia de confidencialidade, autenticidade, integridade, disponibilidade e controle de acesso no ambiente virtual, porém, é necessário conciliar outros recursos com ela para obter-se um melhor resultado, como análises de ameaças, politicas de seguranças e outras ferramentas que visem minimizar o problema que envolve a segurança e dificultar as perdas de informações.

**Palavras Chave:** Redes, Segurança, Informação e Certificação Digital.

## ABSTRACT

Information technology is undergoing a very fast process of evolution and making the lives of its users increasingly accessible, interactive, functional and with unlimited possibilities specially through computer networks that are distributed throughout the world, in which the Internet is helping this process to happen, but with it the need to ensure information security in order to safeguard and maintain the confidentiality of confidential information or even identify computers, people and various devices to provide then access to this content and differentiated services and restricts. The Digital Certification is a solution to the problem of information security in public and private networks, which allows greater assurance of confidentiality, authenticity, integrity, availability and access control in virtual environment, however, it is necessary to reconcile it with other resources to obtain a better result, as analysis of threats, security policies and other tools that aim to minimize the problem involving the safety and hinder the loss of information.

**Keywords:** Networks, Security, Information and Digital Certification.

**SUMÁRIO**

# LISTA DE FIGURAS

# LISTA DE TABELAS

## LISTA DE ABREVEATURAS E SIGLAS

| | |
|---|---|
| **AC** | Autoridade Certificadora |
| **AC-Raiz** | Autoridade Certificadora Raiz |
| **ACT** | Autoridade de Carimbo do Tempo |
| **AR** | Autoridade de Registro |
| **ATM** | Asynchronous Transfer Mode |
| **BACEN** | Banco Central |
| **CEF** | Caixa Econômica Federal |
| **CEI** | Cadastro Específico do INSS |
| **CPF** | Cadastro de Pessoa Física |
| **CG** | Comitê Gestor |
| **CI-NIS** | Contribuinte Individual – Número de Informação Social |
| **CRL** | Certificate Revocation List |
| **COTEC** | Comitê Técnico |
| **CNPJ** | Cadastro Nacional da Pessoa Jurídica |
| **CSS** | Cadastro de Clientes do Sistema Financeiro Nacional |
| **DoS** | Denial of Service |
| **DPC** | Declaração de Práticas de Certificação |
| **e-CAC** | Centro Virtual de Atendimento ao Contribuinte |
| **e-CPF** | Certificado Digital Pessoa Física |
| **e-CNPJ** | Certificado Digital Pessoa Jurídica |

| | |
|---|---|
| **FTP** | File Transfer Protocol |
| **HTTP** | HyperText Transfer Protocol |
| **ICP-Brasil** | Infraestrutura de Chaves Públicas do Brasil |
| **IEC** | International Electrotecnical Comission |
| **IETF** | Internet Engineering Task Force |
| **INSS** | Instituto Nacional do Seguro Social |
| **IP** | Internet Protocol |
| **ITI** | Instituto Nacional da Tecnologia da Informação |
| **ITU-T** | International Telecomunication Union - Telecomunication |
| **ISO** | International Standards Organization |
| **ISO/IEC** | International Standards Organization / International Electrotecnical Comission |
| **ITR** | Imposto Sobre a Propriedade Territorial Rural |
| **LAN** | Local Area Network |
| **LCR** | Lista de Certificados Revogados |
| **MAN** | Metropolitan Area Network |
| **NF-e** | Nota Fiscal Eletrônica |
| **OS** | Politicas de Segurança |
| **OSCP** | Online Certificate Status Protocol |
| **OSI** | Open Systems Interconnection |
| **PCN** | Plano de Continuidade de Negócio |

| | |
|---|---|
| **PER/DCOMP** | Programa Gerador do Pedido de Restituição, Ressarcimento e Reembolso e Declaração de Compensação |
| **PASEP** | Programa de Formação do Patrimônio do Servidor Público |
| **PC** | Políticas de Certificado |
| **PGFN** | Procuradoria Geral da Fazenda Nacional |
| **PIN** | Personal Identification Number |
| **PIS** | Programa de Integração Social |
| **PSS** | Prestadores de Serviços de Suporte |
| **RFB** | Receita Federal do Brasil |
| **SIJUT** | Sistema de Informações Jurídico-Tributárias |
| **SMTP** | Simple Mail Transfer Protocol |
| **SPB** | Sistema de Pagamento Brasileiro |
| **SPED** | Sistema Público de Escrituração Digital |
| **SRF** | Secretária da Receita Federal |
| **TCP** | Transmission Control Protocol |
| **TCP/IP** | Transmission Control Protocol / Internet Protocol |
| **WAN** | Wide Area Network |

## INTRODUÇÃO

A informática vem avançando gradativamente e torna-se cada vez mais comum o relacionamento entre pessoas, computadores, equipamentos e outros através da rede de computadores e principalmente na internet, onde milhões e milhões de pessoas trocam informações pelo mundo todo o dia, seja a trabalho, interatividade, pesquisas e muito mais tornando evidente a necessidade de proteger e garantir a integridade e segurança de parte desse conteúdo através de uma ferramenta que possibilite a confidencialidade e direito de propriedade da informação e atualmente uma das melhores ferramentas para isso é conhecida como “Certificação Digital”.

O **objetivo** deste é proporcionar esclarecimentos sobre a certificação digital e ajudar os usuários a obterem um ambiente mais seguro nas redes de computadores, e também reduzir as perdas de informações principalmente no ambiente da internet através de ferramentas que possibilitem uma melhor segurança da informação.

O capítulo 1 trata das redes de computadores, seus fundamentos, aborda alguns dos principais tipos de redes, tais como: LANs (*Local Area Network*), MANs (*Metropolian Area Network*), WANs (*Wide Area Network*) e ATM (*Asynchronous Transfer Mode*), bem como as definições de protocolo e internet.

Segurança na rede é assunto do capítulo 2 e propõe alguns requisitos básicos a serem adotados para se obter uma melhor segurança no ambiente da rede dentre eles enfoca a confidencialidade, a autenticação, a integridade e a disponibilidade ou controle de acesso.

No capítulo 3 é abordada a segurança da informação e visa garantir a integridade e segurança buscando salvaguardar os direitos de propriedade do detentor da mesma, bem como, mostrar algumas das principais ameaças e uma ferramenta chamada politica de segurança visando reduzir perdas.

A Criptografia é focada no capítulo 4 e ela nos permite dar uma maior segurança à informação, dados, projetos entre outros que necessitam de algum tipo de proteção em função do valor agregado que respectiva possui e para isso é

destacado os dois modelos mais comuns de criptografia utilizados a Simétrica e a Assimétrica.

Certificação digital é assunto do capítulo 5 onde é definido seu significado, bem como os tipos mais comuns de certificados existentes e também é realizado um comparativo entre os principais produtos vendidos pelas duas maiores organizações que efetuam a certificação digital no Brasil. Neste, podem-se encontrar as vantagens em utiliza-la, detalhes sobre o padrão X.509, o período de validade, na prática alguns dos recursos que podem ser utilizados ao portar um certificado digital, os principais responsáveis pela gestão e controle da certificação digital no Brasil nas pessoas da Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs), a infraestrutura de chaves públicas no Brasil (ICP-Brasil), o procedimento para o registro de certificados digitais mais comuns no caso o e-CPF (certificado digital pessoa física) e o e-CNPJ (certificado digital pessoa jurídica), a lista de certificados revogados e seus respectivos modelos.

Exigências e cuidados com segurança na certificação digital está disponível no capítulo 6 e mostram alguns dos critérios de segurança principalmente os físicos a serem abordados e implantados para a realização da certificação digital no Brasil, bem como, alguns cuidados a serem tomados por quem utiliza o mesmo no seu dia-a-dia.

Nas considerações finais é possível verificar o desenrolar e os aspectos importantes observados no decorrer deste projeto principalmente no tocante a redes de computadores, segurança da informação e certificação digital.

# 1 REDES DE COMPUTADORES

Uma rede de computadores consiste em no mínimo dois ou mais computadores conectados com a finalidade de compartilhar dados, informações, serviços, recursos e outras. Algumas características importantes a destacar são as baixas taxas de erros e uma grande capacidade de transmissão de dados chegando facilmente a vários gigabits por segundo e comumente essas redes são de uso restrito ou propriedade privada.

“Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região” (SOARES, 1995, p. 10).

Existem vários tipos de redes de computadores, porém, vamos focar alguns tipos mais convencionais como:

- LANs (*Local Area Network*): são redes de acessos locais e restritos a um determinado ambiente corporativo, educacional, doméstico, etc., isto é, normalmente propriedade privada. Umas das principais finalidades dessas redes são viabilizar a disseminação de dados e informações, além de compartilharem diversos dispositivos e recursos de hardware e software num determinado grupo e permitindo a interação entre os ambientes envolvidos.

> As redes locais, muitas vezes chamadas LANs, são redes privadas contidas em um único prédio ou em um campus universitário com até alguns quilômetros de extensão. Elas são amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais, permitindo o compartilhamento de recursos (por exemplo, impressoras) e a troca de informações. As redes locais têm três características que as diferenciam das demais: (1) tamanho, (2) tecnologia de transmissão e (3) topologia. (TANEMBAUM, 1997, p. 10).

- MANs (*Metropolian Area Network*): são redes semelhantes às LANs que tem um maior alcance e abrangem uma região maior, isto é, interligam diferentes cidades, organizações e outros. Podemos destacar também, que ela possui uma velocidade superior em relação

às LANs em função da necessidade de cobrir uma maior distância e um número maior de usuários.

> Uma rede metropolitana, ou MAN, é, na verdade, uma versão ampliada de uma LAN, pois basicamente os dois tipos de rede utilizam tecnologias semelhantes. Uma MAN pode abranger um grupo de escritórios vizinhos ou uma cidade inteira e pode ser privada ou pública. Esse tipo de rede é capaz de transportar dados e voz, podendo inclusive ser associado à rede de televisão a cabo local. Uma MAN tem apenas dois cabos e não contêm elementos de comutação, capazes de transmitir pacotes através de uma série de linhas de saída. A ausência desses elementos simplifica a estrutura (TANEMBAUM, 1997, p. 12).

- WANs (*Wide Area Network*): são redes que abrangem uma determinada área geográfica, isto é, interligam continentes, países e outros através de satélites, circuitos integrados, etc., são redes de uso público e privado que permitem à transmissão de dados que proporcionam informações, interações e infinitas possibilidades a milhões de usuários ao redor de todo o mundo, como exemplo, podemos citar que um indivíduo no Brasil pode efetuar uma compra no Japão através de apenas uns cliques e esta seria responsável pela transmissão de seus respectivos dados.

> Uma rede geograficamente distribuída, ou WAN, abrange uma grande área geográfica, com frequência um país ou continente. Ela contém um conjunto de máquinas cuja finalidade é executar os programas (ou seja, as aplicações) do usuário. Seguiremos a tradição e chamaremos essas máquinas de host. O termo *end system* também é utilizado na literatura específica. Os hosts estão conectados por uma sub-rede de comunicação ou, simplificando, uma sub-rede. A tarefa da sub-rede é transportar mensagens de um host para outro, exatamente como um sistema de telefonia transporta as palavras da pessoa que fala a que ouve. Essa estrutura de rede é altamente simplificada, pois separa os aspectos da comunicação pertencentes à rede (a sub-rede) dos aspectos de aplicação (os hosts) (TANEMBAUM, 1997, p. 12).

- ATM (*Asynchronous Transfer Mode*): é uma rede orientada a conexões baseada no envio de pacotes de dados padronizados transmitidos por conexões com circuitos virtuais que permitem altas velocidades de transmissão, esses pacotes de dados são chamados de células. Normalmente são utilizados em comutadores de alta velocidade

conectados a outros comutadores, computadores e outros dispositivos, um grande problema encontrado no uso deste é o seu alto custo.

> As redes ATM são orientadas à conexão. Antes de uma chamada ser feita, é preciso enviar uma mensagem para configurar a conexão. Em seguida, todas as células subsequentes seguirão o mesmo caminho em direção a seu destino. A entrega das células não é garantida, mas sua ordem de transmissão é respeitada. Se as células 1 e 2 forem enviadas nessa ordem e ambas conseguirem chegar ao destino, elas chegarão na mesma ordem; a célula 2 nunca chegará antes da célula 1 (TANEMBAUM, 1997, p. 71).

## 1.1 PROTOCOLO

Convencionalmente o relacionamento humano exige alguns protocolos, isto é, boas maneiras, às vezes pedimos “licença ou, por favor,”. O fato a destacar é que existem mensagens específicas que retornam algumas ações desejadas, especificando um pouco melhor, temos uma iteração entre componentes de hardware e software dos computadores e os protocolos tem a finalidade de garantir a integridade dos dados transmitidos, através de mecanismos de relacionamento e retransmissão que determinam o caminho que os pacotes de dados devam percorrer. Como exemplo pode-se se citar os protocolos de roteamento que determinam o caminho de um pacote de dados fonte até o destino, ou até mesmo protocolos de hardware em um adaptador de rede que controlam o fluxo bits sobre os fios que interligam dois computadores.

“O protocolo é um conjunto de regras que controla o formato e o significado dos quadros, pacotes ou mensagens trocadas pelas entidades pares contidas em uma camada” (TANEMBAUM, 1997, p. 31).

Dentre os protocolos destacam-se dois modelos que servem como referência: OSI (*Open Systems Interconnection*) e o TCP/IP (*Transmission Control Protocol / Internet Protocol*).

O modelo OSI não é muito usado nos dias de hoje e não é considerado uma arquitetura de rede, pois não especifica os serviços e os protocolos usados nas suas respectivas camadas. Ele foi uma proposta desenvolvida pela ISO (*International Standards Organization*) com a intenção de padronizar o mesmo, ele apresenta sete camadas, que são:

1. Camada física: é responsável pela transmissão de bits brutos por um canal de comunicação;

2. A camada de enlace de dados: transforma a transmissão bruta em uma linha livre de erros originados pela transmissão;

3. A camada de rede: é responsável pelo controle e operação da sub-rede;

4. A camada de transporte: tem a finalidade de receber dados de uma camada superior, dividir em unidades, repassar essas e assegurar a integridade até outro ponto;

5. A camada de sessão: permite o relacionamento de diferentes usuários e máquinas através de sessões;

6. A camada de apresentação: gerencia a estrutura de dados e permite a relação a um nível mais alto, isto é, sintaxe e semântica;

7. A camada de aplicação: é responsável pelas interações com os usuários, como exemplo, é comumente utilizado no HTTP (*HyperText Transfer Protocol*).

O modelo TCP/IP é altamente difundido em todas as redes de computadores geograficamente distribuídas, isto é, internet mundial e possui quatro camadas que são:

1. A camada de inter-redes: é baseada em uma comutação de pacotes que se relacionam sem interconexões;

2. A camada de transporte: tem o objetivo de permitir que a origem e o destino inter-relacionem entre si, isto é, comuniquem-se;

3. A camada de aplicação: é nela que estão estabelecidos todos os protocolos de nível mais alto (FTP – *File Transfer Protocol*, SMTP – *Simple Mail Transfer Protocol*, HTTP – *HyperText Transfer Protocol*, etc.);

4. A camada de host / rede: é onde host se conecta com a rede permitindo o envio e a recepção de pacotes IP (*Internet Protocol*).

> Os modelos de referência OSI e TCP/IP têm muito em comum. Os dois se baseiam no conceito de uma pilha de protocolos independentes. Além disso, as camadas têm praticamente as mesmas funções. Em ambos os modelos, por exemplo, estão presentes as camadas que englobam até a camada de transporte. Nesses modelos, são oferecidos aos processos que desejam se comunicar um serviço de transporte fim a fim independente do tipo de rede que está sendo usado. Essas camadas formam o provedor de transporte. Mais uma vez ambos os modelos, as camadas acima da camada de transporte dizem respeito aos usuários orientados à aplicação de serviço de transporte (TANEMBAUM, 1997, p. 42).

## 1.2 INTERNET

A internet é uma rede que permite o relacionamento de milhões computadores e dispositivos a nível mundial. Muitos desses dispositivos são formados por computadores pessoais, estações de trabalho, servidores, celulares, entre outros que compartilham informações através de páginas web, arquivos textos, mensagens eletrônicas, etc., eles também são conhecidos como sistemas finais.

“A internet pública é uma rede de computadores mundial, isto é, uma rede que interconecta milhões de equipamentos de comunicação em todo o mundo” (KUROSE E ROSS, 2006, p. 3).

Sistemas finais são conectados por links (enlaces de comunicação) que podem transmitir dados em diferentes taxas de transmissão. Essas sequências de

enlaces de comunicação e comutadores de pacotes transitam desde sua origem até o respectivo destino e são conhecidos como rotas ou caminhos. Normalmente esses tipos de serviços são fornecidos por Provedores de Serviços de Internet (Telefônica, Embratel, NET, etc.) que são meio entre a Internet e os sistemas finais.

Estes sistemas finais possuem dispositivos e equipamentos que executam protocolos que controlam a recepção e envio de dados na internet, e normalmente utilizam o TCP/IP e são padronizados pela IETF (*Internet Engineering Task Force*).

# 2 SEGURANÇA NA REDE

A segurança na rede é um assunto amplamente abordado e muito complexo, em função, dos diversos fatores a serem observados, dentre essas considerações identifica-se as seguintes:

- Confidencialidade tem como objetivo proporcionar acesso da informação somente a quem tiver permissão, isto é, a informação só pode ser acessada por quem tiver a respectiva autorização;

> Confidencialidade. Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida. O fato de abelhudos poderem interceptar a mensagem exige, necessariamente, que seja **cifrada** de alguma maneira (que seus dados sejam disfarçados) para impedir que uma mensagem interceptada seja **decifrada** (entendida) por um interceptador. Esse aspecto de confidencialidade é, provavelmente, o significado mais comumente percebido na expressão comunicação seguro*.* Note, contudo, que essa não é apenas uma definição limitada de comunicação segura, mas também uma definição bastante restrita de *confidencialidade* (KUROSE E ROSS, 2006, p. 513).

- Autenticação atesta a autenticidade da informação visando garantir a identidade de quem encaminhou à respectiva;

> Autenticação. O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação – confirmar que a outra parte realmente é quem alega ser. A comunicação pessoal entre seres humanos resolve facilmente esse problema por reconhecimento visual. Quando entidades comunicantes trocam mensagens por um meio pelo qual não podem ver a outra parte, a autenticação não é assim tão simples. Por que, por exemplo, você deveria acreditar que o e-mail veio a um amigo seu realmente veio daquele amigo? Se alguém o chama ao telefone dizendo ser de seu banco e perguntando qual é o número de sua conta, sua senha e saldo bancário, alegando finalidades de verificação, você daria essas informações? Esperamos que não (KUROSE E ROSS, 2006, p. 513).

- Integridade e não-repudiação de mensagem visa proporcionar uma informação confiável e segura durante o processo de transmissão da informação entre as partes envolvidas de maneira a evitar que uma dessas partes negue a integridade da informação;

> Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também querem asseguram que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão. Extensões das técnicas de soma de verificação que encontramos em protocolos de transporte e de enlace confiáveis podem ser utilizadas para proporcionar integridade à mensagem (KUROSE E ROSS, 2006, p. 513).

- Disponibilidade e controle de acesso dispõem sobre a acessibilidade proporcionando funcionamento contínuo com um bom desempenho e principalmente gerenciando os acessos do respectivo.

> Disponibilidade e controle de acesso. A necessidade imperiosa de segurança na rede ficou dolorosamente óbvia nos últimos anos devido a numerosos ataques de recusa de serviço (*denial of service – DoS*) que inutilizaram uma rede, um hospedeiro, ou qualquer outro componente da infraestrutura de rede, para seus usuários legítimos; o mais notório desses ataques DoS talvez tenha sido o cometido contra os sites Web de inúmeras empresas de alta visibilidade. Portanto, um requisito fundamental para comunicação segura deve ser, antes de mais nada, que ela possa ocorrer – que os 'bandidos' não possam ser legítimos, enquanto outros não levam, naturalmente, á noção de controle de acesso, para garantir que entidades que procuram obter acesso a recursos possam fazê-lo somente se tiverem os direitos de acesso apropriados e realizarem seus acessos de uma maneira bem definida (KUROSE E ROSS, 2006, p. 514).

Estes são alguns dos requisitos básicos para obter uma rede relativamente segura, lembrando que segurança na rede é uma estrutura na qual apenas um elo fraco pode desestruturar todo o contexto de segurança envolvido neste sistema. É necessário entender as vulnerabilidades existentes, assim como, os ataques, as ameaças, as melhores formas de prevenção entre outras buscando ampliar o anglo de visão e criar uma forma mais segura e eficiente de garantir a integridade e confidencialidade da mesma.

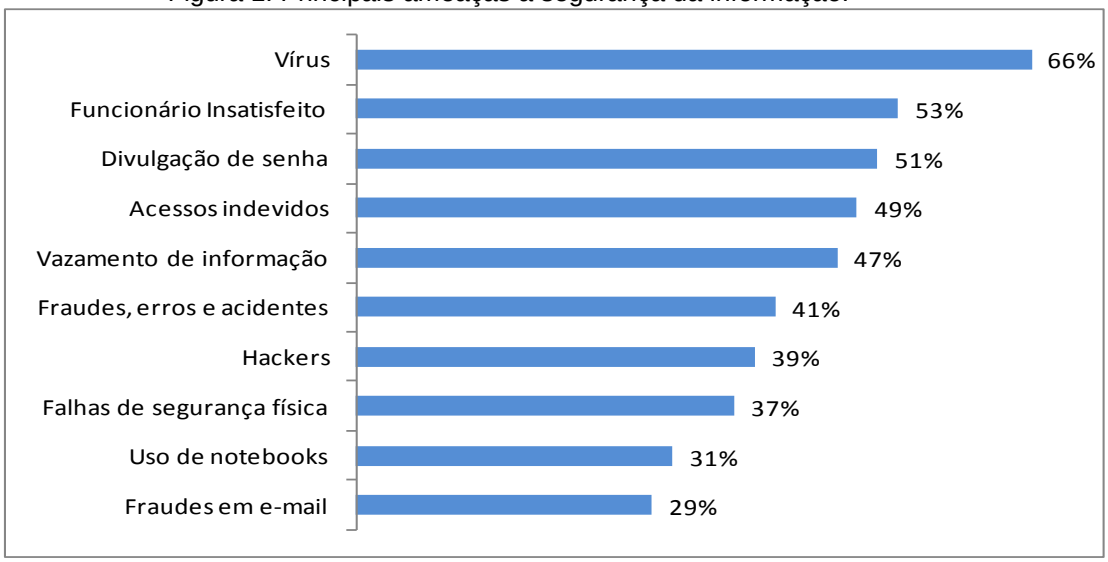
# 3 SEGURANÇA DA INFORMAÇÃO

A premissa principal da segurança da informação é garantir ao responsável que detém a respectiva de inúmeros tipos de ameaças e ataques visando garantir a confidencialidade e integridade da informação proporcionando segurança, maximização da riqueza, domínio de tecnologia e muitos outros, isto é, informações com grande valor agregado pode determinar a vantagem competitiva em um determinado ramo de atividade, setor, mercado de atuação e outros de forma a se tornar um diferencial que pode determinar o sucesso ou fracasso de uma organização.

“O objetivo da segurança da informação é proteger a organização detentora da informação dos diversos tipos de ameaças para garantir a continuidade dos seus negócios e maximizar o retorno dos investimentos e as oportunidades de negócio” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 4).

Atualmente é uma dos assuntos mais abordados entre os especialistas da área de informática em função de sua grande importância e da necessidade principalmente do indivíduo pessoa física ou jurídica de garantir a propriedade da informação buscando salvaguardar o capital intelectual. Porém, existem diversas ameaças que podem comprometer o mesmo, como se pode visualizar na figura abaixo:

Figura 1: Principais ameaças à segurança da informação.




Fonte: MENEZES (2006:28).
Nesta figura acima o total de citações é superior a 100% devido à questão aceitar múltiplas respostas.

"A espionagem empresarial e a contra-espionagem começam, portanto, a desenvolver diferentes mecanismos de proteção para o tráfego das informações, criando consequentemente um ambiente com alto grau de entropia" (MENEZES, 2006, p. 31).

A maior parte desses tipos de vazamentos de informações é causa da espionagem empresarial buscando um caminho mais rápido de conseguir o conhecimento de concorrentes diretos ou indiretos a fim de utiliza-lo em benefício próprio. Imagine como exemplo, conseguir um projeto de um veículo que será lançado por uma montadora de veículos concorrente, bem como, todas as tecnologias e melhorias deste. A organização prejudicada pelas perdas das informações poderá até mesmo perder seu mercado atuante e seus clientes em função da concorrente oferecer os mesmos benefícios e mais alguns, podendo até mesmo em casos mais graves determinar a extinção ou falência da organização lesada. Podemos entender este tipo de caso como uma concorrência desleal, porém, neste mercado cada vez mais competitivo e globalizado a informação passa a ter um valor inestimável e ser de crucial importância manter sua proteção.

> Um firewall não impede o vazamento de dados. O correio eletrônico é de fato a forma mais simples de se enviar dados para fora da empresa, mas também é a forma mais perigosa, já que o tráfego de correio pode ser controlado e auditado. Um espião consciencioso preferirá uma fita, um disquete (razão pela qual há quem defenda o

> banimento dos *drives* de disquete) ou um simples fax. E não existe apólice de seguro contra estupidez, se um funcionário fornecer sua senha de acesso a usuários não autorizados ou desconhecidos, não há *firewall* que resolva (MENEZES, 2006, p. 41).

## 3.1 SEGURANÇA DA INFORMAÇÃO NA INTERNET

A internet é um meio comum utilizado por milhões e milhões de indivíduos, isto é, possui inúmeras variáveis e mecanismos que podem comprometer a segurança da informação, no entanto, existem maneiras de minimizar este problema através de adoção de métodos e soluções tecnológicas que dificultem a perda dessas informações.

### 3.1.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Uma das maneiras mais eficientes é através de uma política de segurança da informação bem elaborada, delimitando o ponto de atuação e as maneiras como devem ser executados alguns métodos e serviços de forma a padronizar e mensurar possíveis problemas futuros, isto é, para obter um ambiente relativamente seguro é essencial que conheça o ambiente interno e externo, assim como, suas respectivas vulnerabilidades, ameaças e outras variáveis que possam ocorrer.

> Uma política de segurança representa as ações que são ou não permitidas durante a operação de um sistema. Uma política de segurança de alto nível leva em consideração a operação segura de um sistema de caráter integral, sem necessariamente prover detalhes de implementação de como os resultados desejados devem ser alcançados. A política de informação representa as considerações gerais em termos mais preciosos dos requisitos de segurança do sistema, passando por um processo de refinamento na especificação do sistema para o qual ela será aplicada (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 6).

# 4 CRIPTOGRAFIA

A criptografia é o estudo de uma informação embaralhada buscando ocultar significado de maneira que somente quem possui sua estrutura pode decifrar o mesmo. Porém, é difícil garantir que somente quem possui a solução pode decifrar, já que atualmente existem várias formas de desvenda-la. No entanto, o valor agregado da informação tende a reduzir com o tempo e a quebra do algoritmo criptográfico consome demasiado tempo para obter a informação de modo não autorizado tendendo aos custos e recursos utilizados para adquiri-la seja bem maior do que a própria informação.

> A palavra criptografia é originária dos termos gregos *kryptós*, que quer dizer oculto, e *graph*, escrever. Em dicionários da língua portuguesa, pode-se encontrar a seguinte definição para palavra criptografia: escrita secreta por meio de abreviaturas ou de sinais convencionados de modo a preservar a confidencialidade da informação (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 13).

## 4.1 CRIPTOGRAFIA SIMÉTRICA

É baseada em uma chave secreta que através de operações (algoritmos) são codificadas e decodificadas, isto é, somente os portadores dessa chave secreta tem acesso à informação, também é conhecida como “Criptografia de Chave Secreta”.

“Criptografia de chave secreta (também chamada de criptografia simétrica) usa uma chave secreta para criptografar uma mensagem de texto cifrado e a mesma chave para decifrar o texto cifrado em texto pleno” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 17).

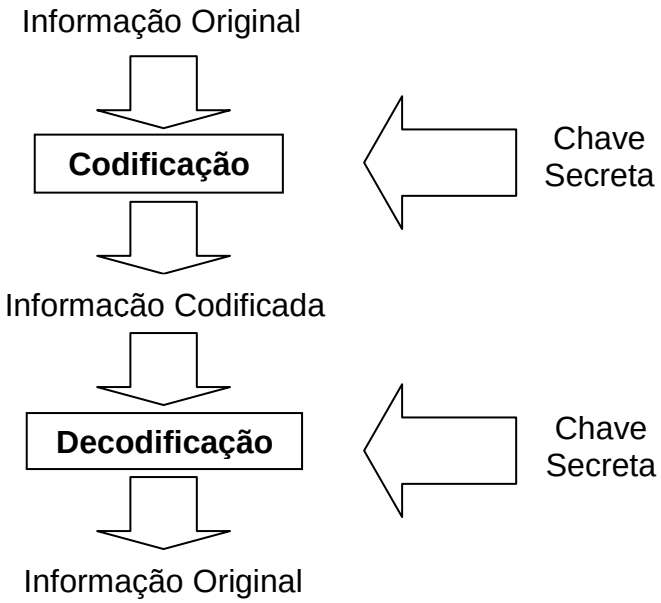



Figura 2: Modelo de codificação e decodificação simétrica.

## 4.2 CRIPTOGRAFIA ASSIMÉTRICA

Este tipo de criptografia também é conhecida como “Criptografia de Chave Pública”, ela trabalha com algoritmos que necessitam de pares de chaves, ou seja, duas partes com chaves diferentes para codificar e decodificar a informação respectivamente. Por exemplo: a chave 1 de um par somente poderá ser decodificada pela chave 2 do mesmo par.

> A criptografia de chave pública (também chamada de criptografia assimétrica) envolve duas chaves distintas, uma pública e uma privada. A chave privada é mantida em segredo e nunca deve ser divulgada. Por outro lado, a chave pública não é secreta e pode ser livremente distribuída e compartilhada com qualquer pessoa (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 18).

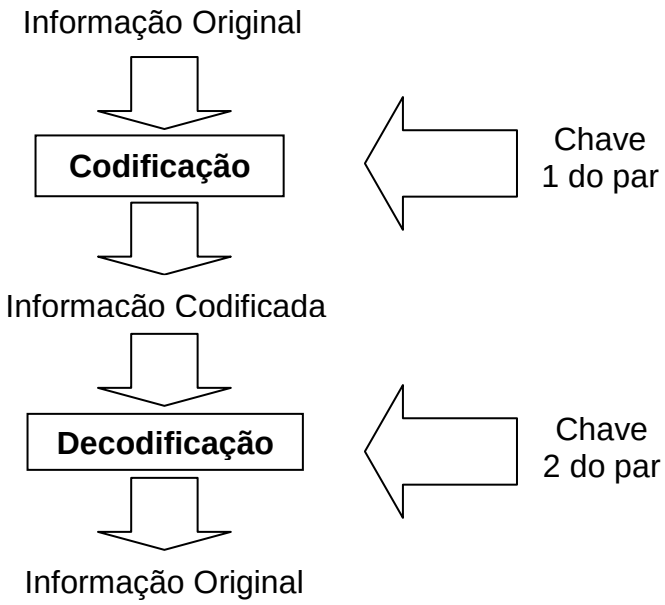



Figura 3: Modelo de codificação e decodificação assimétrica.

# 5 CERTIFICAÇÃO DIGITAL

Atualmente, certificação digital é uma das tecnologias de segurança da informação mais utilizadas, isto é, uma ferramenta essencial surgida em função da necessidade de manter a integridade e segurança da informação, bem como, alimentar o sistema público, permitir uma melhor segurança na interação junto à internet, em fim, assegurar todas as relações eletrônicas.

Certificado digital pode-se ser entendido como um documento digital que visa identificar pessoas, empresas, computadores, aplicações e outras que possam existir de maneira eletrônica que buscam utilizar serviços disponíveis e/ou guardar informações com maior segurança.

> Um certificado digital (também chamado do certificado de chave pública) é uma ligação entre a chave pública de uma entidade e um ou mais atributos relacionados a esta entidade, armazenados em um arquivo digital. O usuário neste caso pode ser uma pessoa, dispositivo de hardware ou um processo de software. O certificado digital produz a garantia que a chave pública pertence à entidade. Além disso, garante também que a entidade (e somente esta entidade) possui de fato a correspondente chave privada (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 26).

## 5.1 TIPOS DE CERTIFICADOS

Existem diversos tipos de certificados digitais que podem ser adquiridos atualmente, no entanto, é necessário saber qual a finalidade de seu uso e principalmente as necessidades do mesmo para obter uma maior segurança e mais apropriada à solução do problema.

Na tabela abaixo podemos encontrar um comparativo entre as duas maiores empresas que prestam serviços de certificação no país com suas respectivas descrições de alguns de seus produtos mais comumente encontrados e utilizados no mercado.

Tabela 1: Comparativo dos certificados

| Tipos de Certificados | Verisign Inc. (Certisign) | Serasa Experian |
|---|---|---|
| **e-CPF** |  O e-CPF é a versão eletrônica do CPF, que garante a autenticidade e a integridade nas transações eletrônicas de pessoas físicas. |  O e-CPF é o seu documento de identificação na internet. Com ele, você pode assinar documentos eletrônicos com validade jurídica, autenticar-se em sites, realizar serviços da Receita Federal, como entrega de declarações e acesso ao e-CAC, tanto para a pessoa física quanto para as empresas das quais você for o representante legal. |
| **e-CNPJ** |  O e-CNPJ é a versão eletrônica do CNPJ, que garante a autenticidade e a integridade nas transações eletrônicas de pessoas jurídicas. |  O e-CNPJ é o documento de identificação da sua empresa. Com ele, você pode assinar documentos eletrônicos com validade jurídica, autenticar-se em sites, realizar serviços da Receita Federal, como entrega de declarações e acessar o e-CAC. |
| **NF-e** |  Criado especialmente para emitir notas fiscais eletrônicas (garantindo sua conformidade na Lei) e atribuir ao funcionário responsável de sua organização a alçada necessária e restrita para emissão e gerenciamento de NF-e. |  A Serasa Experian desenvolveu uma família de certificados digitais para Nota Fiscal Eletrônica (NF-e). Se você emite milhares de notas por dia ou algumas dezenas por mês, temos a solução correta para a sua necessidade. |
| **Servidor Web** |  Possui cifragem de 128 bits e conta com uma excelente relação custo-benefício. Este certificado é adotado como prática de segurança por todos os tipos de organizações para proteger suas aplicações web. |  O Certificado de Servidor é o elo de confiança entre sua empresa e seu cliente, garantindo a credibilidade e autenticidade do seu website. Além disso, todas as informações enviadas por meio do site trafegam de forma segura, criptografadas até o servidor da empresa. |
| **Sistema de Pagamento Brasileiro (SPB)** |  Conecte-se ao Sistema de Pagamentos Brasileiro com a garantia de segurança dos certificados Certisign. |  Para a participação das instituições no Sistema de Pagamento Brasileiro (SPB), o Banco Central determinou uma série de procedimentos de segurança, entre eles a necessidade de certificado digital específico: o Certificado SPB. |
| **CSS** | |  O Certificado CCS garante às instituições financeiras total segurança nas operações no Cadastro de Clientes do Sistema Financeiro Nacional. Toda comunicação com o Banco Central (BACEN) trafega criptografada, atendendo aos rigorosos requisitos de segurança da ICP-Brasil. |

Fontes: Verisign Inc. (Certisign), 2010 / Serasa Experian, 2010.

## 5.2 VANTAGENS DA CERTIFICAÇÃO DIGITAL

A certificação digital beneficia diversas áreas e setores de nossa economia proporcionando uma melhor segurança e integridade da informação e dentre essas vantagens, podem-se destacar:

- Acompanhamento de processos jurídicos online;
- Contribuintes podem acessar informações junto aos órgãos públicos permitindo que renegocie suas dividas, realize cópias de documentos, consiga segunda via de impostos e tributos pagos entre muitas outras;
- Entrega de obrigações principais e acessórias de maneira simplificada e segura;
- Evitar fraudes digitais ocasionados por terceiros;
- Maior segurança na web;
- Maior produtividade, agilidade e competitividade através de um acesso simplificado da informação;
- Redução no volume de papéis oriundos da burocracia por documentos eletrônicos e digitais;
- Redução nas filas intermináveis nas agências, secretarias, repartições públicas e outras organizações governamentais ou não;
- Transmissão de informações no meio eletrônico de maneira segura, garantindo a integridade do mesmo.

Existem muitas outras vantagens que podem ser encontradas através da Certificação Digital e que dependem do ramo de atividade, setores econômicos e tecnológicos, entre outros, assim como, da necessidade e nível de segurança a ser adotado por cada organização, entidade, etc., como já visualizamos no subitem

anterior há várias soluções em certificados para os diferentes tipos necessidades que possam ocorrer e dentre elas escolher a melhor opção para cada caso.

## 5.3 PADRÃO X.509

O padrão X.509 possuem três versões conhecidas e tem sua estrutura definida pela *International Telecomunication Union – Telecomunication* (ITU-T) em parceria com a *ISO/International Electrotecnical Comission* (IEC) que são:

- Versão um: lançada no ano de 1988, com sua estrutura básica.
- Versão dois: lançada no ano de 1993, onde foi implementado o controle de acesso;
- Versão três: lançada no ano de 1996, na qual, disponibilizou a possibilidade de utilizar campos de extensão.

Abaixo temos a tabela 2 que mostra a estrutura da versão três com seus respectivos campos e descrições:

Tabela 2: Descrição dos campos de um certificado no formato X.509 v3.

| NOME DO CAMPO | DESCRIÇÃO |
|---|---|
| Versão | Número da versão X.509 do certificado, tendo como valor válido apenas 1, 2 ou 3. |
| Número de série | Identificador único do certificado e representado por um inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma autoridade certificadora. |
| Algoritmo de assinatura | Identificador do algoritmo usado para a assinatura do certificado pela autoridade certificadora. |
| Emissor | Nome da autoridade certificadora que produziu e assinou um certificado. |
| Período de validade | Intervalo de tempo de duração que determina quando um certificado deve ser considerado válido pelas aplicações. |
| Assunto | Identifica o dono da chave pública do certificado. O assunto deve ser único para cada assunto no certificado emitido por uma autoridade certificadora. |
| Chave Pública | Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada. |

| | |
|---|---|
| Identificador Único de Emissor (opcional) | Campo opcional para permitir o reuso de um emissor com o tempo. |
| Identificador Único de Assunto (opcional) | Campo opcional para permitir o reuso de um assunto com o tempo. |
| Extensões (opcional) | Campos complementares com informações adicionais personalizadas. |

Fonte: Certificação Digital. Conceitos e aplicações, 2008.

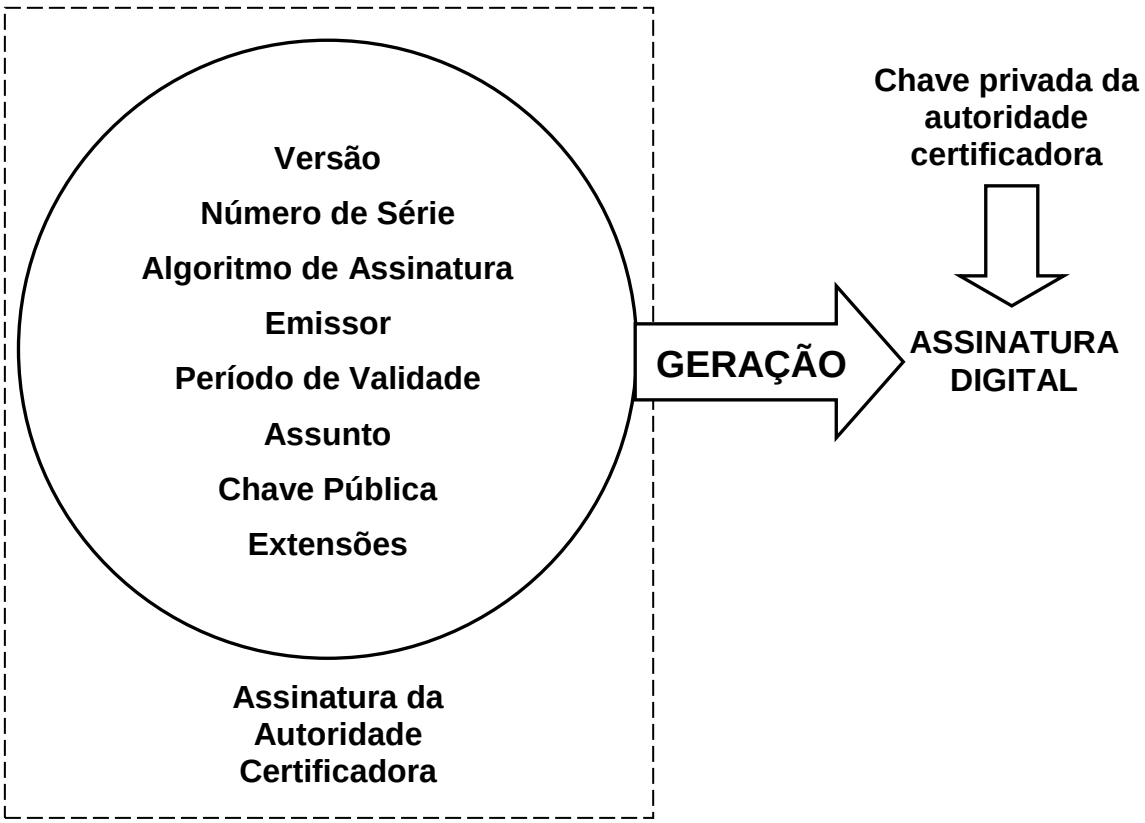
As extensões advindas da versão três permitem um controle mais apurado, no qual, as empresas, autoridades certificadoras entre outros podem efetuar personalizações que se adaptem melhor às suas necessidades. Este campo é dividido em três partes, que são:

- Tipo de extensão: identifica à semântica e o tipo de informação;
- Indicador crítico: padroniza as aplicações de software;
- Valor de extensão: contém o valor real de um campo.

> Um campo de extensão possui três partes: tipo de extensão, indicador crítico e valor de extensão O tipo de extensão é um objeto identificador que provê semântica e tipo de informação (como texto, data, número inteiro ou estrutura complexa) para o valor de extensão. O valor da extensão contém o real valor de um campo de extensão que é descrito pelo seu tipo. O indicador crítico instrui aplicações de software que usam certificados que ignoram o valor do campo quando não se conhece o tipo de extensão. Ao processar um certificado, uma aplicação de software pode seguramente ignorar um campo de extensão não crítica se não reconhecer o tipo de extensão. Por outro lado, deve rejeitar um certificado que contém uma extensão crítica que não reconhece. O indicador crítico permite que aplicações operem com certificados de maneira segura, assim que novas extensões são introduzidas (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 28).

Com base nas informações destacadas acima, podemos visualizar na figura abaixo na parte tracejada todos os campos existentes em um certificado digital, lembrando que não estão inclusos nesta os campos opcionais, já no circulo estão os campos mínimos necessários para a composição de uma assinatura digital. Entretanto vale salientar que todas as partes são necessárias para que o certificado funcione corretamente.

Figura 4: Composição básica de um certificado digital.




## 5.4 PERÍODO DE VALIDADE

Convencionalmente os certificados digitais tem um prazo referente sua vida útil e depois deste período ele é expirado e perde sua funcionalidade, não sendo possível assinar e/ou validar digitalmente qualquer tipo de documento, tendo então, que ser renovado através de procedimentos estabelecidos pelas Autoridades Certificadoras.

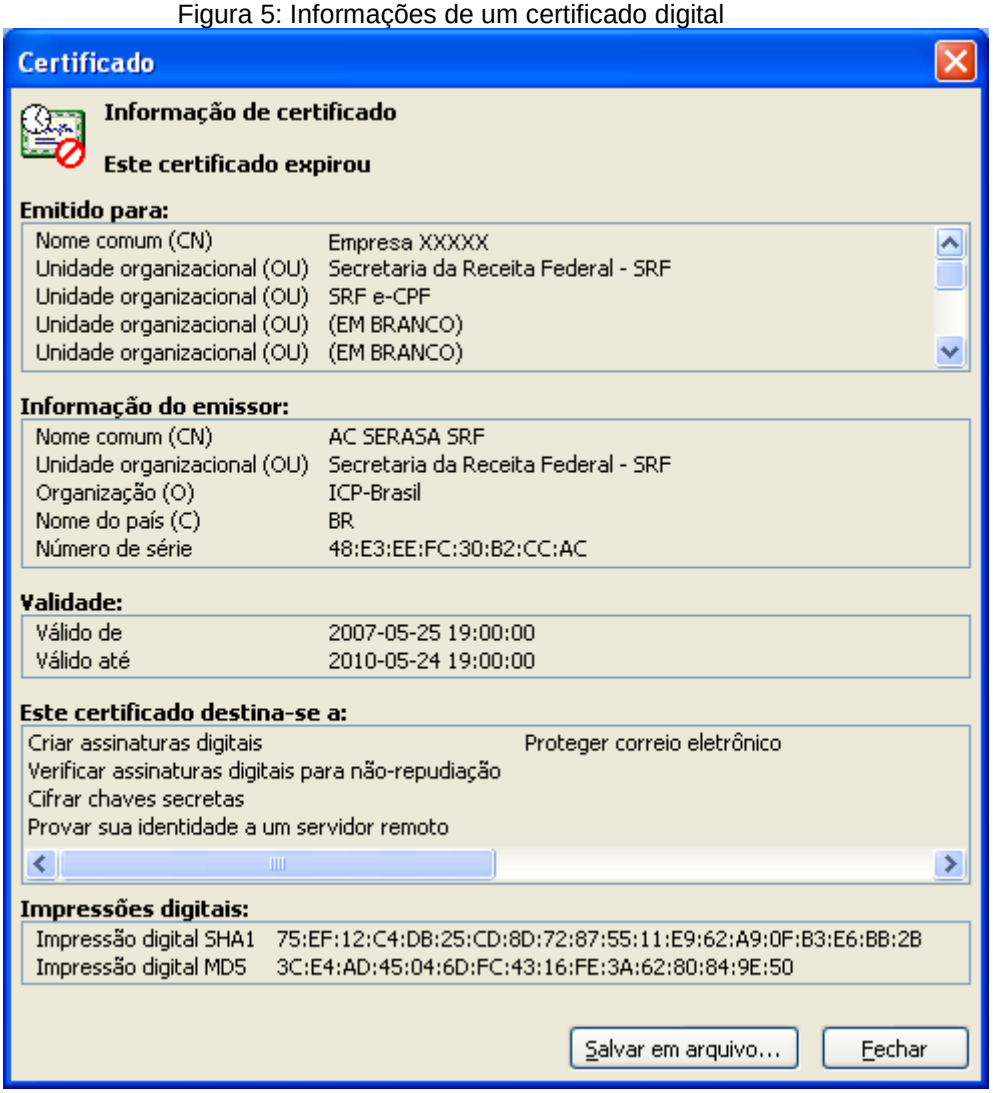
> Um certificado no formato X.509 possui um período de validade, normalmente durando entre alguns meses e alguns anos, durante o qual as aplicações devem aceita-lo. Um certificado é válido por todo o período de validade, depois de terminado este período, é expirado e se torna inválido (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 29).

Empresas como a Serasa Experian e Verisign Inc. (Certisign) utilizam mais comumente a validade de um ano e três anos, porém, esta pode variar de acordo

com a necessidade dos clientes e nível de segurança desejado, podendo ter a validade entre alguns meses até vários anos.

Para verificar a validade de um certificado do tipo A3 da Serasa Experian é necessário ter o mesmo em mãos, além, de instalados os aplicativos que já vem com o certificado digital, a leitora de cartão inteligente e seu respectivo driver (note que existem vários tipos de leitoras de cartão inteligente e esta pode variar de acordo com a disponibilidade da certificadora, tipo do certificado e outros) e através da execução dos processos de instalação que podem ser encontrados no manual do respectivo, ou até mesmo, pelo suporte técnico que as certificadoras disponibilizam. Abaixo na figura, pode-se visualizar um exemplo de consulta das informações de um certificado digital:

Figura 5: Informações de um certificado digital



Com base na figura acima, pode-se verificar que este certificado digital já esta expirado, o nome do titular, o responsável pela emissão, o período de validade, finalidade a que se destina e outras informações relevantes sobre utilização do mesmo.

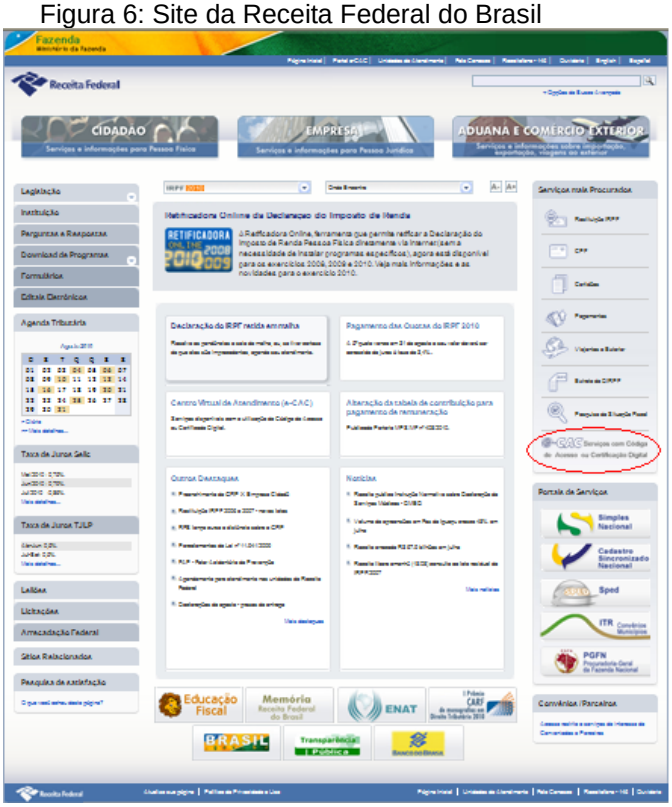
## 5.5 UTILIZANDO UM CERTIFICADO DIGITAL

Um certificado digital tem diversas possibilidades de utilização, porém, para exemplificar melhor e mostrar um pouco na prática como ele funciona, será necessário abordar umas das utilizações mais comuns, no caso, no site da Receita Federal do Brasil (RFB) que disponibiliza vários serviços a fim de simplificar a vida de seus contribuintes.

> Na prática, o certificado digital funciona como uma carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação feita nos meios virtuais, como a rede mundial de computadores - Internet. Tecnicamente, o certificado é um documento eletrônico que por meio de procedimentos lógicos e matemáticos asseguraram a integridade das informações e a autoria das transações (Instituto Nacional da Tecnologia da Informação, 2010).

Primeiramente, deve-se acessar o site da Receita Federal do Brasil (http://www.receita.fazenda.gov.br), no qual, deverá aparecer em seu navegador uma tela semelhante a da figura abaixo.

Figura 6: Site da Receita Federal do Brasil




Fonte: Receita Federal do Brasil, 2010.

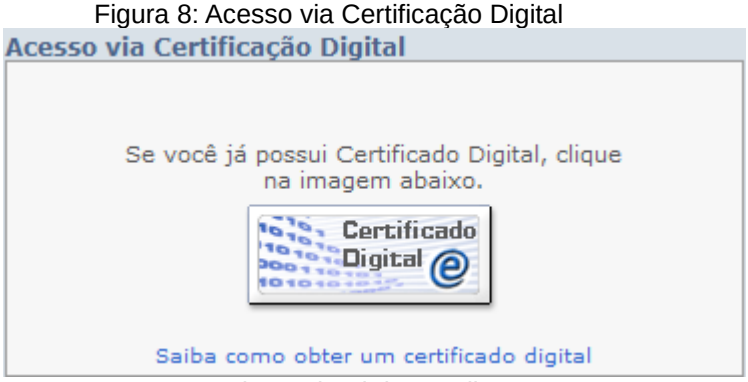
Logo após acessar a opção e-Cac, disponibilizará uma nova página para o acesso com o certificado digital ou Código de Acesso, conforme figura abaixo.

Figura 7: e-CAC


Fonte: Receita Federal do Brasil, 2010.

Selecione a opção Certificado Digital clicando na imagem semelhante a seguir.

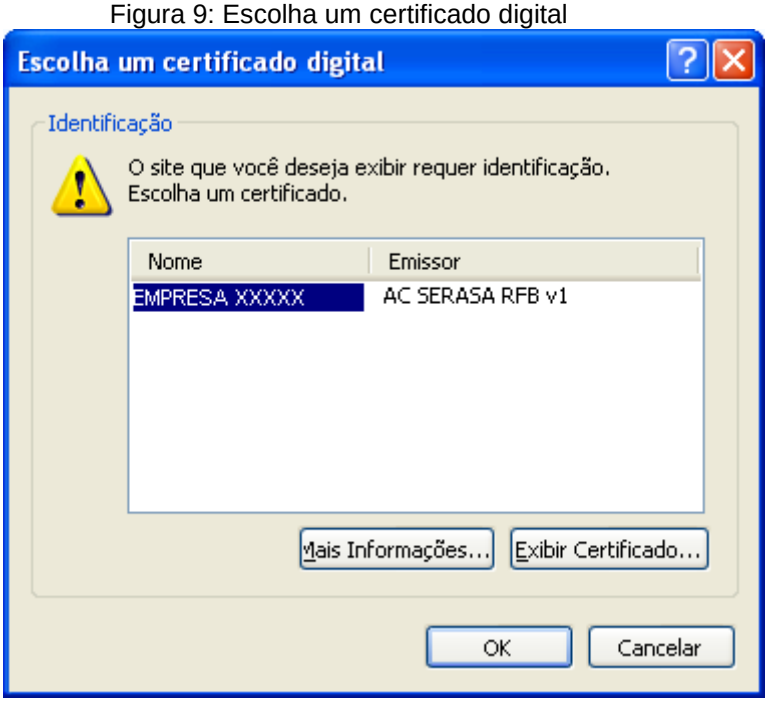
Figura 8: Acesso via Certificação Digital




Fonte: Receita Federal do Brasil, 2010.

Agora tem início a interação com o certificado digital, apecerá uma tela igual a da figura abaixo pedindo para que selecione o certificado digital desejado para permitir o acesso aos serviços disponíveis no site da Receita Federal do Barsil.

Figura 9: Escolha um certificado digital




Fonte: Receita Federal do Brasil, 2010.

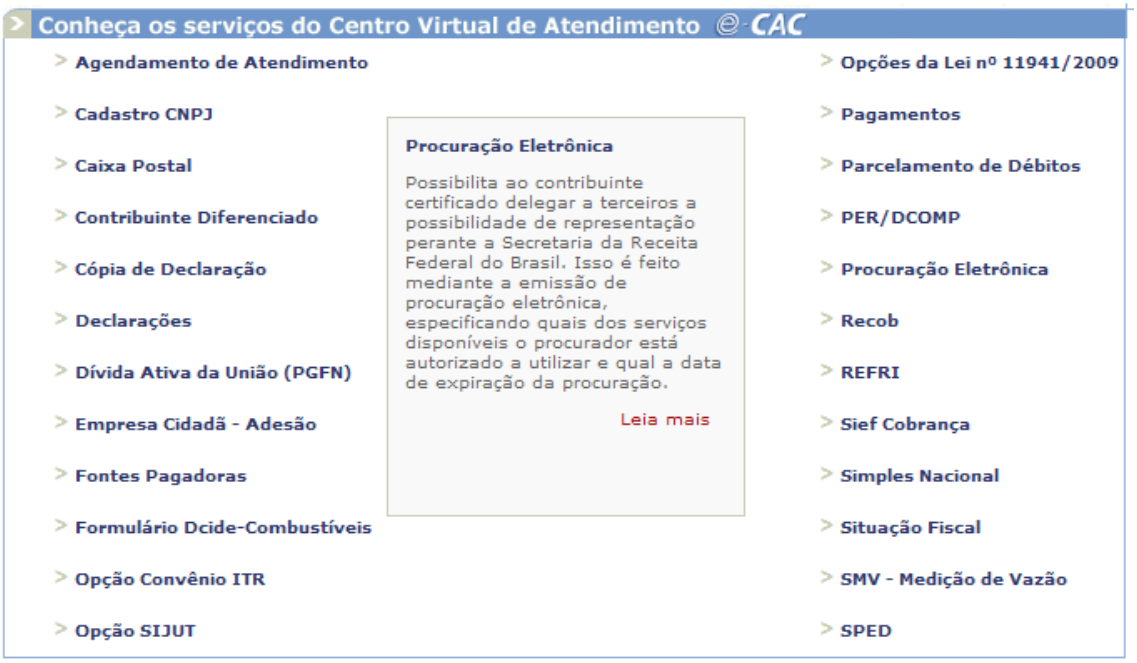
No caso, temos somente um certificado conectado ao computador, então somente um está disponível, porém, em grandes organizações onde há uma estrutura maior podem existir diversas certificações, como por exemplo, departamentos, usuários, aplicações e outros. Agora digite o número do PIN (senha do certificado digital) conforme figura a seguir.

Figura 10: Introduza a senha (PIN) do certificado digital


Fonte: Receita Federal do Brasil, 2010.

Após este último passo, os serviços provenientes do Centro Virtual de Atendimento da Receita Federal do Brasil estarão disponíveis para a utilização conforme figura a seguir.

Figura 11: Serviços disponíveis na Receita Federal do Brasil




Fonte: Receita Federal do Brasil, 2010.

Os serviços disponíveis no Centro Virtual de atendimento da Receita Federal do Brasil são amplamente utilizados por advogados, contadores, auditores, fiscais, peritos e muito outros, porém, vale destacar alguns serviços, como:

- Agendamento de Atendimento: o usuário pode agendar um horário para o atendimento em uma das unidades da Receita Federal;

- Cadastro CNPJ: disponibiliza as organizações consultarem e emitirem o comprovante de inscrição e de situação cadastral de sua empresa;

- Caixa postal: possibilita a recepção de mensagens enviadas pela Receita Federal do Brasil;

- Contribuinte Diferenciado: os contribuintes que tem acompanhamento econômico tributário diferenciado podem acessar e enviar informações através do respectivo;

- Cópia de Declaração: permite adquirir cópia eletrônica de todas as declarações tanto da pessoa jurídica quanto da pessoa física;

- Dívida Ativa da União: consultar todos os débitos inscritos em dívida ativa, parcelar os mesmos, entre outros;

- Empresa Cidadã – Adesão: permite a pessoa jurídica aderir à prorrogação do salário maternidade;

- Fontes Pagadoras: disponibiliza ao usuário imprimir cópia das informações de rendimentos;

- Parcelamento de Débitos: permite ao usuário efetuar parcelamentos relativos a impostos, contribuições federais e outros;

- Procuração Eletrônica: o contribuinte pessoa física ou jurídica pode delegar a um representante legal para que o represente junto a este órgão público através de uma emissão da uma procuração eletrônica;

- Situação Fiscal: permite a pesquisa detalhada de sua situação fiscal, permitindo verificar pendências, problemas diversos, irregularidades e outros para sua respectiva regularização.

Existem muitas outras possibilidades de serviços na Receita Federal do Brasil, porém, foram abordados os mais interessantes e mais utilizados serviços.

Salientando que a maior parte deles visão simplificar a vida do contribuinte, porém, o manuseio inadequado do certificado digital pode significar prejuízos, perdas de informações e outros.

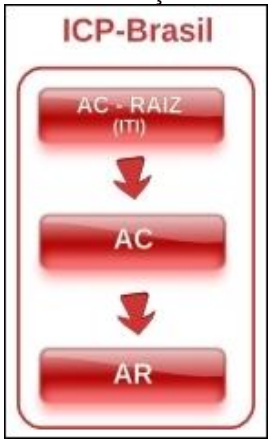
## 5.6 QUEM ESTÁ AUTORIZADO A CERTIFICAR?

Existe uma infraestrutura de chaves públicas na qual o principal responsável pela emissão dos certificados digitais é a Autoridade Certificadora Raiz da ICP-Brasil, no caso, o Instituto Nacional de Tecnologia da Informação (ITI), isto é, é ele quem deverá autorizar as Autoridades Certificadoras e estes por sua vez disponibilizar esta para as Autoridades de Registro, que é onde começa todo o processo através do solicitante da certificação digital.

> O Instituto Nacional de Tecnologia da Informação - ITI é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infra-Estrutura de Chaves Públicas Brasileiras – ICP-Brasil, sendo a primeira autoridade da cadeia de certificação – AC Raiz Internet (Instituto Nacional da Tecnologia da Informação, 2010).

Na figura abaixo se pode ter uma visão mais ampla da hierarquia básica do processo de certificação digital, no caso, na parte mais alta encontra-se a Autoridade Certificadora – Raiz (AC-Raiz), subsequentemente as Autoridades Certificadoras (AC) e na base as Autoridades de Registro (AR).

Figura 12: Modelo de certificação com raiz única.




Fonte: Instituto Nacional de Tecnologia da Informação

### 5.6.1 AUTORIDADE CERTIFICADORA RAIZ

A Autoridade Certificadora Raiz é a principal responsável pelo gerenciamento e geração dos pares de chaves criptográficas e certificações digitais, mais não somente isso, ela também tem outras atribuições, tais como: emissão, expedição e distribuição de certificados para as Autoridades Certificadoras de nível subsequente ao seu; a publicar os certificados emitidos pela mesma; a revogar tais certificados; a emitir e gerenciar a publicação de sua Lista de Certificados Revogados (LCR); a fiscalizar e a auditar as Autoridades Certificadoras, as Autoridades de Carimbo do Tempo (ACTs), as Autoridades de Registro (ARs) e os Prestadores de Serviço de Suporte (PSS); a implementar acordos de certificação cruzada; a adotar medidas de segurança e controle; a manter os processos, procedimentos e atividades em conformidade com a legislação vigente, normas, práticas e regras estabelecidas pelo Comitê Gestor (ICP-Brasil); a manter e garantir a integridade, o sigilo e a segurança da informação e a manter e testar regularmente seu Plano de Continuidade de Negócio (PCN).

> A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu (Instituto Nacional da Tecnologia da Informação, 2010).

### 5.6.2 AC – AUTORIDADE CERTIFICADORA

As Autoridades Certificadoras tem o mesmo objetivo e as responsabilidades atribuídas a Autoridade Certificadora Raiz, porém, estas estão subordinadas a mesma e sujeitas a prestar contas, no entanto, o principal diferencial é que elas a distribuem os certificados para as Autoridades de Registro que estão em um nível subsequente ao seu na hierarquia.

> Uma Autoridade Certificadora é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais.

> Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada) (Instituto Nacional da Tecnologia da Informação, 2010).

### 5.6.3 AR - AUTORIDADE DE REGISTRO

As Autoridades de Registro encontram-se na base de toda hierarquia do processo de certificação digital e estão obrigadas a controlar através de registros todas as suas operações. Elas são o ponto de partida na solicitação da certificação digital, pois são elas os responsáveis pela recepção e encaminharem toda a documentação dos solicitantes as Autoridades Certificadoras.

> Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota (Instituto Nacional da Tecnologia da Informação, 2010).

### 5.6.4 INFRAESTRUTURA DE CHAVES PÚBLICAS

A infraestrutura de chaves públicas no Brasil (ICP-Brasil) foi desenvolvida pelo governo federal brasileiro com o intuito de regularizar a certificação digital no país e também de agilizar os processos decorrentes de operações eletrônicas proporcionando uma melhor segurança e mais simples interação. Ela possui diversas entidades relacionadas, normas regulamentadoras, práticas e princípios a serem abordados, padrões a serem seguidos entre outros.

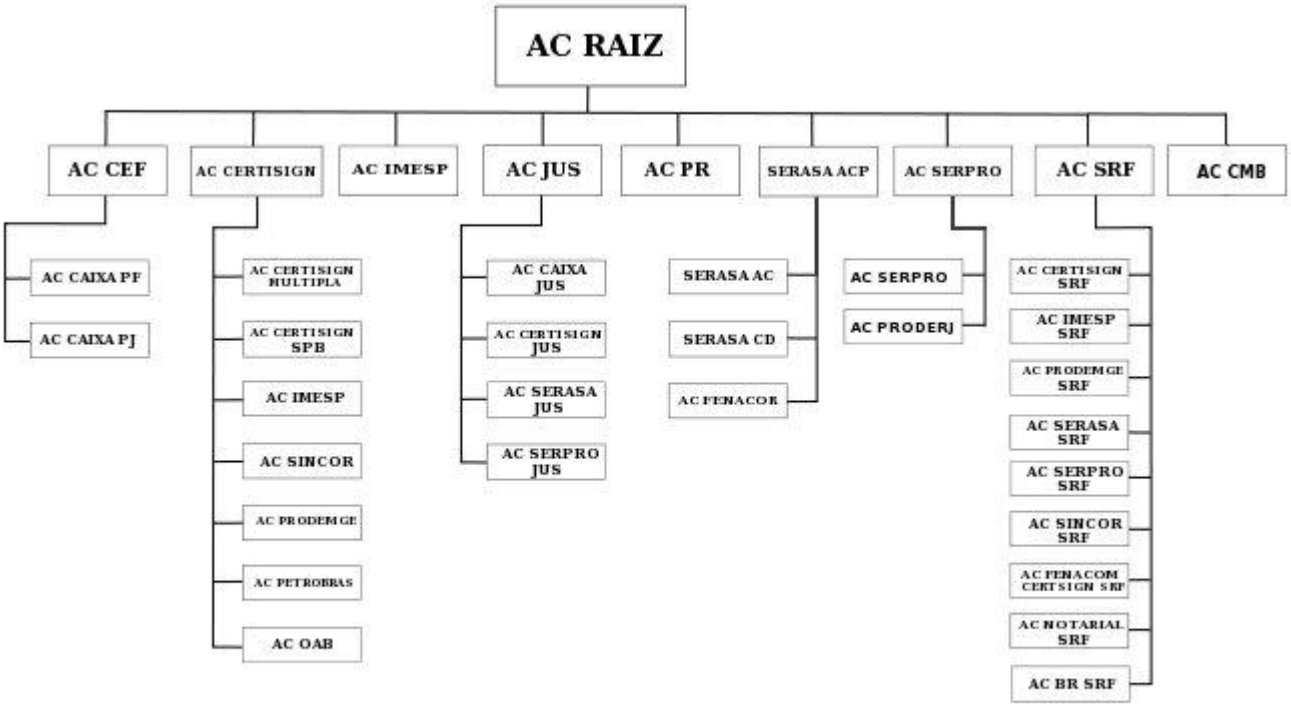
No Brasil a principal característica adotada pela ICP-Brasil é a certificação centralizada em uma única raiz que permite o controle e gerenciamento de todo o

processo que envolve a certificação digital e cabe a ela também fiscalizar, auditar, supervisionar todos os envolvidos nesta hierarquia.

> Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI além de desempenhar o papel de Autoridade Certificadora Raiz - AC Raiz, também, tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos (Instituto Nacional da Tecnologia da Informação, 2010).

Esta estrutura hierárquica apresenta uma cadeia, na qual predomina a confiança de forma a viabilizar o controle e identificação das partes envolvidas.

Figura 13: Infra-Estrutura de Chaves Pública Brasileira (ICP-Brasil)




Fonte: Instituto Nacional de Tecnologia da Informação, 2010.

A figura acima possui um formato árvore, no qual, todos estão subordinados ao topo dela e também uma organização linear devido ao fato que existem linhas diretas e únicas de autoridade e responsabilidade, adaptando-se ao esquema e apresentar características fundamentais, tais como: autoridade, ser linear e única com linhas formais de comunicação, centralização das decisões, entre outros.

> A hierarquia existe para assegurar que as pessoas executem as tarefas e deveres que lhes foram designados. Ela caracteriza por estabelecer, na estrutura organizacional, a relação de subordinação existente, ou seja, uma cadeia de comando, que vem a ser uma linha contínua de autoridade que integra o trabalho as pessoas. A hierarquia está associada ao princípio da unidade de comando que determina que cada indivíduo, ou grupos de indivíduos deve receber ordens de apenas um chefe (MORAES, 2000, p. 93).

A Medida Provisória 2.200-2, de 24 de agosto de 2001 criou diversas entidades com específicas funções e atividades a serem desempenhadas por elas, algumas dessas são realizadas dentro ou não da própria Autoridade Certificadora Raiz da ICP-Brasil, tais como:

- Comitê Gestor (CG): responsável pelo controle e aplicação das políticas e normas técnicas;

- Comitê Técnico (COTEC): responsável por toda a parte técnica envolvida;

- Autoridade Certificadora Raiz (AC-Raiz): responsável pela execução, fiscalização, auditoria e outros. Ela está no topo da hierarquia da certificação digital;

- Autoridades Certificadoras (AC): subordinada a AC-Raiz são encarregadas de gerenciar os certificados (emitir, revogar, etc.) a um nível imediatamente inferior;

- Autoridades de Registro (AR): responsável pelo gerenciamento operacional entre o solicitante e as Autoridades Certificadoras;

- Prestador de Serviços de Suporte (PSS): são contratados pelas Autoridades Certificadoras ou Autoridades de Registro para disponibilização de recursos físicos, lógicos e especializados;

- Auditorias Independentes: são contratadas pela Autoridade Certificadora Raiz para realizarem inspeções operacionais, técnicas, lógicas nas organizações de nível inferior ao dela;

- Titulares de Certificados: são os solicitantes da certificação digital, estão relacionados diretamente com as Autoridades de Registro;

- Terceiras Partes: são partes que podem ser designadas pelas Autoridades Certificadoras a disponibilizarem ou desempenharem algum tipo de função.

Dessas diversas entidades citadas acima vale salientar que tem que passar por um processo de credenciamento rigoroso, no qual, estabelece normas, procedimentos técnicos e medidas para que sejam permitidos a elas exercerem determinadas atividades, podendo ser revogadas a qualquer momento, caso as mesmas não sejam cumpridas e observadas.

> No âmbito da ICP-Brasil, a Resolução n.º 40 do Instituto Nacional de Tecnologia da Informação (ITI), de 18 de abril de 2006, estabelece os critérios e procedimentos a serem observados para o credenciamento, manutenção do credenciamento e descredenciamento de AC, AR e de prestador de serviços de suporte (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 86).

### 5.6.5 REGISTRANDO CERTIFICADOS

O registro de um certificado digital envolve dois pontos cruciais o primeiro é a criação de um par chaves, no caso, a chave pública e a chave privada e posteriormente o envio da chave pública à Autoridade Certificadora, para que esta consiga validar a operação através de um sistema criptográfico, no qual, sempre irá requisitar uma senha para que a respectiva validação seja realizada.

> Os passos de geração da chave pública e privada, a transferência da chave pública para uma AC e a transferência da chave privada para o dono são essenciais durante o registro de certificados. O dono pode gerar o par de chaves em algum tipo de sistema local, armazenar a chave privada e mandar a chave pública utilizando a aplicação, para a AC. O armazenamento da chave pública envolve criptografia, fazendo com que a senha seja requisitada toda vez que precisar ser usada (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 30).

Existe um rigoroso processo para que se consiga realizar a criação de um par de chaves, no qual, as Autoridades de Registro são responsáveis por sua execução, mais comumente são requeridos o e-CPF (certificado digital pessoa física) e o e-CNPJ (certificado digital pessoa jurídica). Nestes casos, é utilizado um cadastro online, onde, o solicitante ou responsável o preenche, efetua sua impressão, assina-o, anexam os documentos necessários e dirigisse a um ponto de atendimento.

Para emissão do e-CPF é obrigatória à apresentação dos seguintes documentos originais com a entrega respectivas cópias:

- Cédula de identidade atualizada ou documento com fé pública no território nacional;
- Cadastro de Pessoa Física (CPF);
- Comprovante de endereço recente;
- Uma foto 3x4 recente;
- Termo de Titularidade do Certificado Digital impresso em duas vias (lembrando que este deve ser assinado no momento da validação presencial);
- Comprovante de inscrição no PIS/PASEP/CI-NIS (Opcional);
- Título de eleitor (Opcional);
- Cadastro específico do INSS-CEI (Opcional);

No caso do preenchimento de um e-CNPJ faz necessário à apresentação de todos os documentos exigidos no e-CPF, no caso, do responsável pela organização, entidade, etc., mais os seguintes:

- Documento de constituição (estatuto, contrato social, requerimento de empresário, atas, etc.) com respectiva comprovação do responsável;

- Cartão do Cadastro Nacional de Pessoa Jurídica (CNPJ);
- Inscrição no Cadastro Específico do INSS (Opcional).

## 5.7 LISTA DE CERTIFICADOS REVOGADOS (LCR)

A lista de certificados revogados é um repositório onde se obtém informações referentes aos certificados digitais, no caso das Autoridades Certificadoras da ICP – Brasil utilizam as LCRs básicas. No entanto, dependendo do crescimento da lista a tendência será a implantação de novos modelos de lista, tais como:

- Lista de Certificados Revogados Sobre-emitidas;
- Lista de Certificados Revogados Segmentadas;
- Lista de Certificados Revogados Delta;
- OCSP.

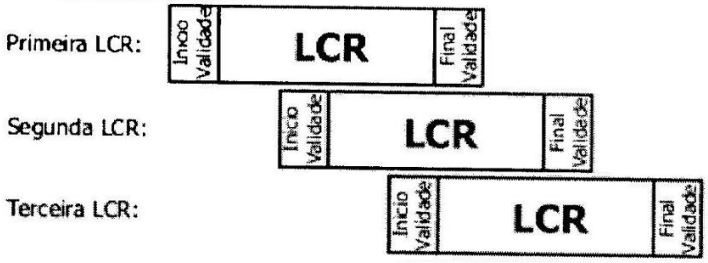
> O modelo básico de emissão de listas de certificados revogados tem algumas características que podem comprometer o desempenho tanto do repositório, que disponibiliza a lista, quanto do usuário, que faz o download da lista para verificar a revogação de algum certificado (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 32).

### 5.7.1 MODELO BÁSICO E SOBRE-EMITIDAS

O modelo Sobre-emitidas possui os mesmos atributos e extensões do modelo básico, o que diferencia uma da outra é apenas a forma como ela é emitida. Para explicar melhor na lista do modelo básico só pode ser emitido quando a lista anterior estiver com o prazo expirado e na lista do modelo sobre-emitidas se deve emitir antes do vencimento do prazo de validade da lista anterior, este por sua vez permite

evitar gargalos na requisição no repositório, tornando o processo mais rápido e eficiente.

Figura 14: Modelo Sobre-emitidas

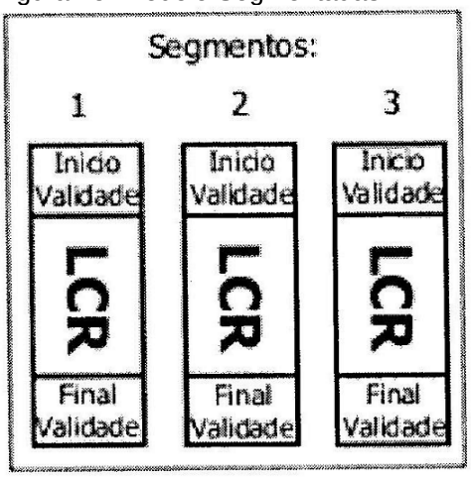



Fonte: Certificação Digital, 2010.

### 5.7.2 MODELO SEGMENTADAS

O modelo Segmentadas também apresenta uma estrutura semelhante ao modelo básico, porém, ela possui o desmembramento em partes que permite a diminuição do tamanho da lista. Estes segmentos quando divididos em repositórios devem conter no campo de extensão o preenchimento do endereço da parte da lista relacionada e assim por diante. A vantagem desse método é a divisão da carga da lista em diversos repositórios, tornando o mesmo mais balanceado.

Figura 15: Modelo Segmentadas




Fonte: Certificação Digital, 2010.

### 5.7.3 MODELO DELTA

O modelo Delta tem objetivo de manter as listas mais atualizadas sem diminuir demasiadamente a eficiência dos repositórios, no entanto, este modelo não apresenta um ganho real, pois, o comportamento da carga de requisições não é muito diferente do modelo básico, além, da frequência maior com que são feitas as requisições, porém, existe uma vantagem, na qual, se o solicitante tiver a lista salva, o mesmo pode obter informações mais atualizadas sem necessariamente baixar a lista completa novamente.

Tabela 3: Modelo Delta

| CLR Base | CLR Delta |
|---|---|
| Publicação = 00:00<br>Próxima Publicação = 06:00<br>N. da CRL = 1 | Publicação = 00:00<br>Próxima Publicação = 02:00<br>N. da CRL = 1 |
| | Publicação = 02:00<br>Próxima Publicação = 04:00<br>N. da CRL = 1 |
| | Publicação = 04:00<br>Próxima Publicação = 06:00<br>N. da CRL = 1 |
| Publicação = 06:00<br>Próxima Publicação = 12:00<br>N. da CRL = 4 | Publicação = 06:00<br>Próxima Publicação = 08:00<br>N. da CRL = 1 |
| | Publicação = 08:00<br>Próxima Publicação = 10:00<br>N. da CRL = 4 |
| | Publicação = 10:00<br>Próxima Publicação = 12:00<br>N. da CRL = 4 |

Fonte: Certificação Digital, 2010.

### 5.7.4 OCSP

O modelo OCSP permite a verificação online da lista de certificados revogados e funciona através de um processo de requisições que consultam um ou mais banco de dados e depois retornam uma mensagem em conformidade com os padrões definidos e pode facilmente suprir algumas das necessidades encontradas, em função, da sua maior simplicidade e facilidade de uso proporciona redução no tempo para verificação, outra vantagem é que se consulta apenas o certificado desejado, isto é, não precisa baixar a lista inteira. Porém, a mesma é dependente de

um servidor que disponibiliza este serviço, além dos outros serviços agregados (internet, telefonia, provedor, etc.) que também possuem um limite que pode ocasionar atrasos indesejáveis, esta não é indicada para ambientes sem acesso a internet.

“Este modelo de verificação pode substituir as listas de certificados revogados em alguns casos. Por ser um modelo online, o tempo entre o pedido de revogação e a obtenção desta informação pelos interessados em verificar o certificado é reduzido” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 37).

# 6 EXIGÊNCIAS E CUIDADOS COM CERTIFICAÇÃO DIGITAL

Na ICP Brasil podem-se encontrar os procedimentos e diretrizes com respeito à segurança na certificação digital para as Autoridades Certificadoras (AC) e estes devem ser seguidos rigorosamente pela as mesmas, tais como:

- Declaração de Práticas de Certificação (DPC): cita os procedimentos práticos e de certificação que devem ser seguidos pela autoridade certificadora;

- Políticas de Certificado (PC): cita as políticas e normas de um denominado certificado digital elaborado por uma autoridade certificadora.

- Políticas de Segurança (OS): cita as principais diretrizes de segurança abordadas pela Autoridade Certificadora.

Estas medidas de seguranças definidas para Autoridades Certificadoras possuem controle físico, humano, lógico e de recursos criptográficos definidos em níveis de segurança, dentre eles vale a pena salientar que o aspecto físico exige um nível de segurança extraordinário em seis níveis que são:

- Nível um: propõe a criação de uma barreira para às instalações internas, isto é, identificação e controle de acesso de pessoal através de segurança qualificada e devidamente armada;

“O primeiro nível – ou nível um deve-se situar-se após a primeira barreira de acesso às instalações da AC. Para entrar em uma área de segurança nível um, cada indivíduo deverá ser identificado e registrado por segurança armada” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 54).

- Nível dois: todos os usuários devem novamente apresentar identificação e passar por um novo controle de acesso, este é o nível

onde serão realizados os processos administrativos e operacionais de menor relevância;

“O segundo nível – ou nível dois – é interno ao primeiro e deve requerer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse será o nível mínimo de segurança requerido para a realização de qualquer processo operacional ou administrativo AC” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 54).

- Nível três: aqui cada indivíduo deve passar por um rigoroso processo de identificação, no qual, deve-se controlar e registrar as entradas e saídas dos mesmos através de dispositivo eletrônico, de preferência, utilizar identificação biométrica, e também não é permitido possuir qualquer tipo de equipamento eletrônico, tais como: celulares, relógios, pendrives, etc. exceto o essencial para execução do processo. A partir deste nível que serão encontrados as documentações referentes os certificados digitais;

“O terceiro nível – ou nível três – deve-se situar-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais deverá estar localizada a partir desse nível” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 55).

- Nível quatro: toda a estrutura física deve ser reforçada através de paredes revestidas com material de alta densidade (aço, concreto, etc.) de tal forma que não permita saída de qualquer elemento (água, vapor, fogo, etc.) e entrada física através da ventilação e refrigeração, além, de seguir as mesmas orientações do nível três e também devem seguir as normas brasileiras aplicáveis as salas-cofre das instituições financeiras do Brasil. Neste nível é onde serão realizadas as operações referentes ao certificado digital e devem-se permanecer no mínimo duas pessoas na execução destes processos.

“No quarto nível (nível quatro), interior ao terceiro, é onde devem ocorrer atividades especialmente sensíveis das operações da AC, tais como emissão e revogação de certificados, e emissão de LCRs” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 55).

- Nível cinco: dentro do nível quatro deve existir um cofre, armário ou gabinete reforçado que permita a inserção de documentos e materiais de criptografia da Autoridade Certificadora;

“O quinto nível (nível cinco), interior aos ambientes de nível quatro, deve compreender um cofre ou gabinete reforçado trancado” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 56).

- Nível seis: dentro do cofre, armário ou gabinete deve conter divisórias com fechadura individual disponibilizando local para a colocação dos dados de ativação da Autoridade Certificadora.

“O sexto nível (nível seis) deve consistir de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos deve dispor de fechadura individual” (AQUINO JUNIOR, BATISTA, HOMOLKA, LIMA, CAETANO DA SILVA E CORDEIRO DA SILVA, 2008, p. 56).

As Autoridades Certificadoras subordinadas a Autoridade Certificadora Raiz, constantemente passam por auditorias e fiscalizações que avaliam os aspectos que envolvem a segurança e caso encontrem irregularidades estes terão seus certificados revogados até que regularizarem a respectiva situação.

Para quem pretende adquirir um certificado digital primeiramente deve-se analisar a finalidade para qual vai adquiri-lo buscando sempre a melhor escolha, isto é, buscar saciar suas necessidades sem exageros levando em consideração o melhor custo benefício, bem como, a melhor solução. Para isso, faz-se necessário ás vezes a busca de um especialista da área da informática.

Grandes e médias organizações possuem regulamentos e práticas que especificam bem quais os cuidados a serem tomados e como seus funcionários devem se comportar quando o manusear ou estiver de posse do respectivo, ou mesmo, nas auditorias internas ou externas que costumam dar uma atenção especial sobre este assunto, porém, em algumas pequenas organizações ou usuários comuns não tem esse tipo de cuidado, até mesmo, às vezes por ter um ambiente familiar, para tanto, colocaremos algumas das práticas de segurança mais comuns a todos aos usuários que podem evitar problemas relacionados com o certificado digital, tais como:

- Somente o titular da chave privada deve manusear e utilizar o certificado digital, pois, todas as transações realizadas serão em nome dele;

- Não compartilhar a senha do certificado digital com ninguém e principalmente utilizar uma senha longa com caracteres maiúsculos, minúsculos e números dificultando que programas possam desvendar o mesmo;

- Caso a chave criptográfica possua materialidade guardar em local apropriado que somente o titular do cartão tenha acesso. Se for armazenado no disco rígido do computador o que não é aconselhável, procurar limitar através de senhas ou outras formas de segurança que limitem o acesso de outros indivíduos. Se estiver compartilhado em uma rede privada limitar para que somente esses indivíduos envolvidos tenham acesso, isto é, não deixar que todos os usuários dessa rede tenham acesso ao mesmo, e assim por diante, tentar buscar sempre a melhor solução para a segurança do respectivo.

Muitos usuários de certificado digital não dão as devidas importâncias ao armazenamento adequado e usabilidade do mesmo, ocasionado muitos prejuízos, pois, não entendem que uma assinatura digital corresponde a uma assinatura com reconhecimento de firma e acabam descobrindo quando já é tarde demais ou quando terceiros se aproveitam e o usam indevidamente. Portanto, é necessário

manter seu certificado digital em local seguro e adotar algumas práticas e procedimentos de segurança que visem melhorar, selecionar, manusear de maneira mais adequada o respectivo.

# 7 CONSIDERAÇÕES FINAIS

Redes de computadores tem a finalidade de possibilitar o relacionamento e interação a fim de facilitar o acesso à informação seja numa rede privada ou pública, isto é, visa o compartilhamento de informação entre dispositivos, computadores, pessoas entre outros que se relacionam entre si. Atualmente, está muito difundido principalmente o uso da internet que permite o acesso a um ilimitado conteúdo, a maior parte destes na figura de pessoas que já utilizaram ou utilizam direta ou indiretamente as diversas possibilidades disponibilizadas por esse meio de comunicação inovador que tende a cada vez mais se tornar acessível, interativo, funcional e ilimitado.

Segurança é um assunto que preocupa a todos em todas as esferas públicas ou privadas no Brasil, e neste caso, com o ambiente virtual não é diferente, pois, faz-se necessário tomar precauções para não perder informações cruciais e importantes que possam possibilitar a terceiros: vantagens competitivas, financeiras, gerenciais e muitas outras. Na era digital a informação pode valer ouro e nas mãos erradas podem ser utilizadas de forma errada e causar grandes prejuízos a organizações, entidades, pessoas e a todos que dependem dela. Por isso, é essencial utilizar a tecnologia a nosso favor a fim de tornar o ambiente virtual protegido e um lugar mais seguro, no qual, as partes possam utiliza-la para desempenhar suas atividades e processos sem medo de ocorrer perdas e prejuízos sejam eles financeiros, tecnológicos, morais entre outros.

Certificação Digital atualmente é uma das principais ferramentas utilizadas para garantir a segurança, integridade, identidade da informação envolvida. Ela possibilita diversas formas concretas para isso, o mundo se torna cada vez mais digital e com ele a necessidade de saber o que é real ou não, quem é quem e muito mais. Por isso, uma das formas mais lógicas para obter-se: confidencialidade, autenticidade, integridade, disponibilidade e controle de acesso nas redes de computadores por todo o mundo e principalmente garantir as partes que participam deste é a certificação digital, mais somente isso não resolve, é necessário junto com ela estabelecer politicas de segurança da informação, criptografias, análises de

ameaças e muito mais visando minimizar este problema de segurança e dificultar ao máximo a perda de informações.

# 8 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. Citação**: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

AQUINO JUNIOR, IVANILDO JOSÉ DE SOUZA; BATISTA, EDUARDO MAZZA; HOMOLKA, HEBERT OTTO; LIMA, MARCELO FERREIRA DE; SILVA, LUIZ GUSTAVO CORDEIRO DA. E SILVA, PAULO EDUARDO DA. **Certificação Digital - Conceitos e Aplicações - Modelos Brasileiro e Australiano.** 1ª ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

CERTISIGN. Disponível em http://www.certisign.com.br/. Acesso em: 07 de junho de 2010 às 10:54.

ITI – Instituto Nacional da Tecnologia da Informação. Disponível em http://www.iti.gov.br/. Acesso em: 24 de agosto de 2010 às 08:29.

KUROSE, JAMES F e ROSS, KEITH W. **Redes de Computadores e a Internet.** 3ª ed. São Paulo: Editora Pearson Addison Wesley, 2006.

MENEZES, JOSUÉ DAS CHAGAS. **Gestão da Segurança da Informação.** 1ª ed. Campinas: Editora J. H. Mizuno, 2006.

MORAES, Anna Maris Pereira. Iniciação ao Estudo da Administração. 2ª Ed. São Paulo: Makron Books, 2000.

RECEITA FEDERAL DO BRASIL. Disponível em http://www.receita.fazenda.gov.br. Acesso em 25 de agosto de 2010 às 10:45.

SERASA EXPERIAN. Disponível em http://www.certificadodigital.com.br. Acesso em 07 de junho de 2010 às 11:04.

SOARES, Luiz Fernando Gomes; LEMOS, Guido e COLCHER, Sérgio. **Redes de Computadores.** 2ª ed. Rio de Janeiro: Editora Campus, 1995.

TANEMBAUM, ANDREW S. **Redes de Computadores.** 3ª ed. Rio de Janeiro: Editora Campus, 1997.