Cartilha de Segurança para Internet

Parte I: Conceitos de Segurança

Versão 3.0
Setembro de 2005
http://cartilha.cert.br/

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte I: Conceitos de Segurança

Esta parte da Cartilha apresenta conceitos de segurança de computadores, onde são abordados temas relacionados às senhas, engenharia social, *malware*, vulnerabilidade, ataques de negação de serviço, criptografia e certificados digitais. Os conceitos aqui apresentados são importantes para o entendimento de partes subseqüentes desta Cartilha.

Versão 3.0 – Setembro de 2005
http://cartilha.cert.br/

Sumário

1 Segurança de Computadores

Um computador (ou sistema computacional) é dito seguro se este atende a três requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade.

A confidencialidade diz que a informação só está disponível para aqueles devidamente autorizados; a integridade diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto, e a disponibilidade diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários.

Alguns exemplos de violações a cada um desses requisitos são:

Confidencialidade: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda;

Integridade: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal;

Disponibilidade: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

1.1 Por que devo me preocupar com a segurança do meu computador?

Computadores domésticos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de produtos e serviços; comunicação, por exemplo, através de *e-mails*; armazenamento de dados, sejam eles pessoais ou comerciais, etc.

É importante que você se preocupe com a segurança de seu computador, pois você, provavelmente, não gostaria que:

- suas senhas e números de cartões de crédito fossem furtados e utilizados por terceiros;
- sua conta de acesso a Internet fosse utilizada por alguém não autorizado;
- seus dados pessoais, ou até mesmo comerciais, fossem alterados, destruídos ou visualizados por terceiros;
- seu computador deixasse de funcionar, por ter sido comprometido e arquivos essenciais do sistema terem sido apagados, etc.

1.2 Por que alguém iria querer invadir meu computador?

A resposta para esta pergunta não é simples. Os motivos pelos quais alguém tentaria invadir seu computador são inúmeros. Alguns destes motivos podem ser:

- utilizar seu computador em alguma atividade ilícita, para esconder a real identidade e localização do invasor;

- utilizar seu computador para lançar ataques contra outros computadores;
- utilizar seu disco rígido como repositório de dados;
- destruir informações (vandalismo);
- disseminar mensagens alarmantes e falsas;
- ler e enviar *e-mails* em seu nome;
- propagar vírus de computador;
- furtar números de cartões de crédito e senhas bancárias;
- furtar a senha da conta de seu provedor, para acessar a Internet se fazendo passar por você;
- furtar dados do seu computador, como por exemplo, informações do seu Imposto de Renda.

2 Senhas

Uma senha (*password*) na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, é utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser.

Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você na Internet. Alguns dos motivos pelos quais uma pessoa poderia utilizar sua senha são:

- ler e enviar *e-mails* em seu nome;
- obter informações sensíveis dos dados armazenados em seu computador, tais como números de cartões de crédito;
- esconder sua real identidade e então desferir ataques contra computadores de terceiros.

Portanto, a senha merece consideração especial, afinal ela é de sua inteira responsabilidade.

2.1 O que não se deve usar na elaboração de uma senha?

Nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas[1] deverão estar **fora** de sua lista de senhas. Esses dados podem ser facilmente obtidos e uma pessoa mal intencionada, possivelmente, utilizaria este tipo de informação para tentar se autenticar como você.

Existem várias regras de criação de senhas, sendo que uma regra muito importante é **jamais** utilizar palavras que façam parte de dicionários. Existem *softwares* que tentam descobrir senhas combinando e testando palavras em diversos idiomas e geralmente possuem listas de palavras (dicionários) e listas de nomes (nomes próprios, músicas, filmes, etc.).

[1] Qualquer data que possa estar relacionada com você, como por exemplo a data de seu aniversário ou de familiares.

2.2 O que é uma boa senha?

Uma boa senha deve ter pelo menos oito caracteres[2] (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar.

Normalmente os sistemas diferenciam letras maiúsculas das minúsculas, o que já ajuda na composição da senha. Por exemplo, "`pAraleLepiPedo`" e "`paRalElePipEdo`" são senhas diferentes. Entretanto, são senhas fáceis de descobrir utilizando *softwares* para quebra de senhas, pois não possuem números e símbolos, além de conter muitas repetições de letras.

2.3 Como elaborar uma boa senha?

Quanto mais "bagunçada" for a senha melhor, pois mais difícil será descobrí-la. Assim, tente misturar letras maiúsculas, minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase qualquer e pegar a primeira, segunda ou a última letra de cada palavra.

Por exemplo, usando a frase "batatinha quando nasce se esparrama pelo chão" podemos gerar a senha "`!BqnsepC`" (o sinal de exclamação foi colocado no início para acrescentar um símbolo à senha). Senhas geradas desta maneira são fáceis de lembrar e são normalmente difíceis de serem descobertas.

Mas lembre-se: a senha "`!BqnsepC`" deixou de ser uma boa senha, pois faz parte desta Cartilha.

Vale ressaltar que se você tiver dificuldades para memorizar uma senha forte, é preferível anotá-la e guardá-la em local seguro, do que optar pelo uso de senhas fracas.

2.4 Quantas senhas diferentes devo usar?

Procure identificar o número de locais onde você necessita utilizar uma senha. Este número deve ser equivalente a quantidade de senhas **distintas** a serem mantidas por você. Utilizar senhas diferentes, uma para cada local, é extremamente importante, pois pode atenuar os prejuízos causados, caso alguém descubra uma de suas senhas.

Para ressaltar a importância do uso de senhas diferentes, imagine que você é responsável por realizar movimentações financeiras em um conjunto de contas bancárias e todas estas contas possuem a mesma senha. Então, procure responder as seguintes perguntas:

- Quais seriam as conseqüências se alguém descobrisse esta senha?
- E se fossem usadas senhas diferentes para cada conta, caso alguém descobrisse uma das senhas, um possível prejuízo teria a mesma proporção?

[2] Existem serviços que permitem utilizar senhas maiores do que oito caracteres. Quanto maior for a senha, mais difícil será descobrí-la, portanto procure utilizar a senha de maior tamanho possível.

2.5 Com que freqüência devo mudar minhas senhas?

Você deve trocar suas senhas regularmente, procurando evitar períodos muito longos. Uma sugestão é que você realize tais trocas a cada dois ou três meses.

Procure identificar se os serviços que você utiliza e que necessitam de senha, quer seja o acesso ao seu provedor, *e-mail*, conta bancária, ou outro, disponibilizam funcionalidades para alterar senhas e use regularmente tais funcionalidades.

Caso você não possa escolher sua senha na hora em que contratar o serviço, procure trocá-la com a maior urgência possível. Procure utilizar serviços em que você possa escolher a sua senha.

Lembre-se que trocas regulares são muito importantes para assegurar a confidencialidade de suas senhas.

2.6 Quais os cuidados especiais que devo ter com as senhas?

De nada adianta elaborar uma senha bastante segura e difícil de ser descoberta, se ao usar a senha alguém puder vê-la. Existem várias maneiras de alguém poder descobrir a sua senha. Dentre elas, alguém poderia:

- observar o processo de digitação da sua senha;
- utilizar algum método de persuasão, para tentar convencê-lo a entregar sua senha (vide seção 4.1);
- capturar sua senha enquanto ela trafega pela rede.

Em relação a este último caso, existem técnicas que permitem observar dados, à medida que estes trafegam entre redes. É possível que alguém extraia informações sensíveis desses dados, como por exemplo senhas, caso não estejam criptografados (vide seção 8).

Portanto, alguns dos principais cuidados que você deve ter com suas senhas são:

- certifique-se de não estar sendo observado ao digitar a sua senha;
- não forneça sua senha para qualquer pessoa, em hipótese alguma;
- não utilize computadores de terceiros (por exemplo, em *LAN houses*, *cybercafes*, *stands* de eventos, etc) em operações que necessitem utilizar suas senhas;
- certifique-se que seu provedor disponibiliza serviços criptografados, principalmente para aqueles que envolvam o fornecimento de uma senha.

2.7 Que cuidados devo ter com o usuário e senha de *Administrator* (ou *root*) em um computador?

O usuário *Administrator* (ou *root*) é de extrema importância, pois detém todos os privilégios em um computador. Ele deve ser usado em situações onde um usuário normal não tenha privilégios para

realizar uma operação, como por exemplo, em determinadas tarefas administrativas, de manutenção ou na instalação e configuração de determinados tipos de *software*.

Sabe-se que, por uma questão de comodidade e principalmente no ambiente doméstico, muitas pessoas utilizam o usuário *Administrator* (ou *root*) para realizar todo e qualquer tipo de atividade. Ele é usado para se conectar à Internet, navegar utilizando o *browser*, ler *e-mails*, redigir documentos, etc.

Este é um procedimento que deve ser **sempre evitado**, pois você, como usuário *Administrator* (ou *root*), poderia acidentalmente apagar arquivos essenciais para o funcionamento do sistema operacional ou de algum *software* instalado em seu computador. Ou ainda, poderia instalar inadvertidamente um *software* malicioso que, como usuário *Administrator* (ou *root*), teria todos os privilégios que necessitasse, podendo fazer qualquer coisa.

Portanto, alguns dos principais cuidados que você deve ter são:

- elaborar uma boa senha para o usuário *Administrator* (ou *root*), como discutido na seção 2.3, e seguir os procedimentos descritos na seção 2.6;
- utilizar o usuário *Administrator* (ou *root*) somente quando for estritamente necessário;
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador, para substituir assim o usuário *Administrator* (ou *root*) em tarefas rotineiras, como leitura de *e-mails*, navegação na Internet, produção de documentos, etc.

3 *Cookies*

Cookies são pequenas informações que os *sites* visitados por você podem armazenar em seu *browser*. Estes são utilizados pelos *sites* de diversas formas, tais como:

- guardar a sua identificação e senha quando você vai de uma página para outra;
- manter listas de compras ou listas de produtos preferidos em *sites* de comércio eletrônico;
- personalizar *sites* pessoais ou de notícias, quando você escolhe o que quer que seja mostrado nas páginas;
- manter a lista das páginas vistas em um *site*, para estatística ou para retirar as páginas que você não tem interesse dos *links*.

A parte III: Privacidade apresenta alguns problemas relacionados aos *cookies*, bem como algumas sugestões para que se tenha maior controle sobre eles.

4 Engenharia Social

O termo é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

4.1 Que exemplos podem ser citados sobre este método de ataque?

Os dois primeiros exemplos apresentam casos onde foram utilizadas mensagens de *e-mail*. O último exemplo apresenta um ataque realizado por telefone.

Exemplo 1: você recebe uma mensagem *e-mail*, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.

Exemplo 2: você recebe uma mensagem de *e-mail*, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um *site* da Internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

Exemplo 3: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigí-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso a Internet e, portanto, relacionando tais atividades ao seu nome.

Estes casos mostram ataques típicos de engenharia social, pois os discursos apresentados nos exemplos procuram **induzir** o usuário a realizar alguma tarefa e o **sucesso** do ataque depende única e exclusivamente da **decisão** do usuário em fornecer informações sensíveis ou executar programas.

A parte IV: Fraudes na Internet apresenta algumas formas de se prevenir deste tipo de ataque.

5 Vulnerabilidade

Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Existem casos onde um *software* ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável.

A parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção apresenta algumas formas de identificação de vulnerabilidades, bem como maneiras de prevenção e correção.

6 Códigos Maliciosos (*Malware*)

Código malicioso ou *Malware* (***Mal**icious Soft**ware***) é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Na literatura de segurança o termo *malware* também é conhecido por "*software* malicioso".

Alguns exemplos de *malware* são:

- vírus;
- *worms* e *bots*;
- *backdoors*;
- cavalos de tróia;
- *keyloggers* e outros programas *spyware*;
- *rootkits*.

A parte VIII: Códigos Maliciosos (*Malware*) apresenta descrições detalhadas e formas de identificação e prevenção para os diversos tipos de código malicioso.

7 Negação de Serviço (*Denial of Service*)

Nos ataques de negação de serviço (DoS – *Denial of Service*) o atacante utiliza **um** computador para tirar de operação um serviço ou computador conectado à Internet.

Exemplos deste tipo de ataque são:

- gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;
- gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível;
- tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários a suas caixas de correio no servidor de *e-mail* ou ao servidor *Web*.

7.1 O que é DDoS?

DDoS (*Distributed Denial of Service*) constitui um ataque de negação de serviço distribuído, ou seja, **um conjunto** de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Normalmente estes ataques procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

7.2 Se uma rede ou computador sofrer um DoS, isto significa que houve uma invasão?

Não. O objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadí-los. É importante notar que, principalmente em casos de DDoS, computadores comprometidos podem ser utilizados para desferir os ataques de negação de serviço.

Um exemplo deste tipo de ataque ocorreu no início de 2000, onde computadores de várias partes do mundo foram utilizados para indisponibilizar o acesso aos *sites* de algumas empresas de comércio eletrônico. Estas empresas não tiveram seus computadores comprometidos, mas sim ficaram impossibilitadas de vender seus produtos durante um longo período.

8 Criptografia

Criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:

- autenticar a identidade de usuários;
- autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
- proteger a integridade de transferências eletrônicas de fundos.

Uma mensagem codificada por um método de criptografia deve ser **privada**, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser **assinada**, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de identificar se uma mensagem pode ter sido modificada.

Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais **chaves**. A chave é uma seqüência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens.

Atualmente, os métodos criptográficos podem ser subdivididos em duas grandes categorias, de acordo com o tipo de chave utilizada: a criptografia de chave única (vide seção 8.1) e a criptografia de chave pública e privada (vide seção 8.2).

8.1 O que é criptografia de chave única?

A criptografia de chave única utiliza a mesma chave tanto para codificar quanto para decodificar mensagens. Apesar deste método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens, tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas.

Exemplos de utilização deste método de criptografia e sugestões para o tamanho mínimo da chave única podem ser vistos nas seções 8.4 e 8.5, respectivamente.

8.2 O que é criptografia de chaves pública e privada?

A criptografia de chaves pública e privada utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens. Neste método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Seja o exemplo, onde José e Maria querem se comunicar de maneira sigilosa. Então, eles terão que realizar os seguintes procedimentos:

1. José codifica uma mensagem utilizando a chave pública de Maria, que está disponível para o uso de qualquer pessoa;
2. Depois de criptografada, José envia a mensagem para Maria, através da Internet;
3. Maria recebe e decodifica a mensagem, utilizando sua chave privada, que é apenas de seu conhecimento;
4. Se Maria quiser responder a mensagem, deverá realizar o mesmo procedimento, mas utilizando a chave pública de José.

Apesar deste método ter o desempenho bem inferior em relação ao tempo de processamento, quando comparado ao método de criptografia de chave única (seção 8.1), apresenta como principal vantagem a livre distribuição de chaves públicas, não necessitando de um meio seguro para que chaves sejam combinadas antecipadamente. Além disso, pode ser utilizado na geração de assinaturas digitais, como mostra a seção 8.3.

Exemplos de utilização deste método de criptografia e sugestões para o tamanho mínimo das chaves pública e privada podem ser vistos nas seções 8.4 e 8.5, respectivamente.

8.3 O que é assinatura digital?

A assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

Desta forma, é utilizado o método de criptografia de chaves pública e privada, mas em um processo inverso ao apresentado no exemplo da seção 8.2.

Se José quiser enviar uma mensagem assinada para Maria, ele codificará a mensagem com sua chave privada. Neste processo será gerada uma assinatura digital, que será adicionada à mensagem enviada para Maria. Ao receber a mensagem, Maria utilizará a chave pública de José para decodificar a mensagem. Neste processo será gerada uma segunda assinatura digital, que será comparada à primeira. Se as assinaturas forem idênticas, Maria terá certeza que o remetente da mensagem foi o José e que a mensagem não foi modificada.

É importante ressaltar que a segurança do método baseia-se no fato de que a chave privada é conhecida apenas pelo seu dono. Também é importante ressaltar que o fato de assinar uma mensagem

não significa gerar uma mensagem sigilosa. Para o exemplo anterior, se José quisesse assinar a mensagem e ter certeza de que apenas Maria teria acesso a seu conteúdo, seria preciso codificá-la com a chave pública de Maria, depois de assiná-la.

8.4 Que exemplos podem ser citados sobre o uso de criptografia de chave única e de chaves pública e privada?

Exemplos que combinam a utilização dos métodos de criptografia de chave única e de chaves pública e privada são as conexões seguras, estabelecidas entre o *browser* de um usuário e um *site*, em transações comerciais ou bancárias via *Web*.

Estas conexões seguras via *Web* utilizam o método de criptografia de chave única, implementado pelo protocolo SSL (*Secure Socket Layer*). O *browser* do usuário precisa informar ao *site* qual será a chave única utilizada na conexão segura, antes de iniciar a transmissão de dados sigilosos.

Para isto, o *browser* obtém a chave pública do certificado[3] da instituição que mantém o *site*. Então, ele utiliza esta chave pública para codificar e enviar uma mensagem para o *site*, contendo a chave única a ser utilizada na conexão segura. O *site* utiliza sua chave privada para decodificar a mensagem e identificar a chave única que será utilizada.

A partir deste ponto, o *browser* do usuário e o *site* podem transmitir informações, de forma sigilosa e segura, através da utilização do método de criptografia de chave única. A chave única pode ser trocada em intervalos de tempo determinados, através da repetição dos procedimentos descritos anteriormente, aumentando assim o nível de segurança de todo o processo.

8.5 Que tamanho de chave deve ser utilizado?

Os métodos de criptografia atualmente utilizados, e que apresentam bons níveis de segurança, são publicamente conhecidos e são seguros pela robustez de seus algoritmos e pelo tamanho das chaves que utilizam.

Para que um atacante descubra uma chave ele precisa utilizar algum método de força bruta, ou seja, testar combinações de chaves até que a correta seja descoberta. Portanto, quanto maior for a chave, maior será o número de combinações a testar, inviabilizando assim a descoberta de uma chave em tempo hábil. Além disso, chaves podem ser trocadas regularmente, tornando os métodos de criptografia ainda mais seguros.

Atualmente, para se obter um bom nível de segurança na utilização do método de criptografia de chave única, é aconselhável utilizar chaves de no mínimo 128 bits. E para o método de criptografia de chaves pública e privada é aconselhável utilizar chaves de 2048 bits, sendo o mínimo aceitável de 1024 bits. Dependendo dos fins para os quais os métodos criptográficos serão utilizados, deve-se considerar a utilização de chaves maiores: 256 ou 512 bits para chave única e 4096 ou 8192 bits para chaves pública e privada.

[3] Certificados são discutidos na seção 9 e na parte IV: Fraudes na Internet.

9 Certificado Digital

O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Este arquivo pode estar armazenado em um computador ou em outra mídia, como um *token* ou *smart card*.

Exemplos semelhantes a um certificado digital são o CNPJ, RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a instituição ou pessoa e a autoridade (para estes exemplos, órgãos públicos) que garante sua validade.

Algumas das principais informações encontradas em um certificado digital são:

- dados que identificam o dono (nome, número de identificação, estado, etc);
- nome da Autoridade Certificadora (AC) que emitiu o certificado (vide seção 9.1);
- o número de série e o período de validade do certificado;
- a assinatura digital da AC.

O objetivo da assinatura digital no certificado é indicar que uma outra entidade (a Autoridade Certificadora) garante a veracidade das informações nele contidas.

9.1 O que é Autoridade Certificadora (AC)?

Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

Os certificados digitais possuem uma forma de assinatura eletrônica da AC que o emitiu. Graças à sua idoneidade, a AC é normalmente reconhecida por todos como confiável, fazendo o papel de "Cartório Eletrônico".

9.2 Que exemplos podem ser citados sobre o uso de certificados?

Alguns exemplos típicos do uso de certificados digitais são:

- quando você acessa um *site* com conexão segura, como por exemplo o acesso a sua conta bancária pela Internet (vide parte IV: Fraudes na Internet), é possível checar se o *site* apresentado é realmente da instituição que diz ser, através da verificação de seu certificado digital;
- quando você consulta seu banco pela Internet, este tem que se assegurar de sua identidade antes de fornecer informações sobre a conta;
- quando você envia um *e-mail* importante, seu aplicativo de *e-mail* pode utilizar seu certificado para assinar "digitalmente" a mensagem, de modo a assegurar ao destinatário que o *e-mail* é seu e que não foi adulterado entre o envio e o recebimento.

A parte IV: Fraudes na Internet apresenta algumas medidas de segurança relacionadas ao uso de certificados digitais.

Como Obter este Documento

Este documento pode ser obtido em http://cartilha.cert.br/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@cert.br.

Nota de *Copyright* e Distribuição

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.