GLOSSÁRIO ICP-BRASIL

Versão 1.2

03.10.2007

PALAVRA CHAVE	DESCRIÇÃO
ABNT (Associação Brasileira de Normas Técnicas)	Fundada em 1940, é o órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro.
Aceitação do Certificado Digital	Demonstração da concordância de uma pessoa física ou jurídica quanto à correção e adequação do conteúdo e de todo o processo de emissão de um certificado digital, feita pelo indivíduo ou entidade que o solicitou. O certificado é considerado aceito a partir de sua primeira utilização, ou após haver decorrido o prazo pré-estipulado para sua rejeição. A aceitação do certificado será declarada pelo titular.
Acesso	Estabelecimento de conexão entre um indivíduo ou entidade e um sistema de comunicação ou de informações. A partir do Acesso podem ocorrer a transferência de dados e a ativação de processos computacionais.
Acesso Físico	Habilidade de obter acesso a um ambiente físico. Os sistemas de controle de Acesso Físico possibilitam a integração de funcionalidades, com leitores biométricos, alarmes de incêndio, emissão de crachás para visitantes, etc.
Acesso lógico	O Controle de Acesso Lógico permite que os sistemas de Tecnologia da Informação verifiquem a identidade dos usuários que tentam utilizar seus serviços. Como exemplo mais comum, temos o *logon* de um usuário em um computador.
Acesso Remoto	Habilidade de obter acesso a um computador ou uma rede a distância. As conexões *dial-up, wireless*, DSL são exemplos de possibilidades de Acesso Remoto.
AES (Advanced Encryption Standard)	O Padrão de Cifração Avançada (AES) é uma cifra de bloco adotada como padrão de cifração pelo governo dos Estados Unidos. O AES é um dos algoritmos mais populares usados na criptografia de chave simétrica. AES tem um tamanho de bloco fixo de 128 bits e uma chave com tamanho de 128, 192 ou 256 bits.
Agente de Registro	Responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a autenticação da identidade de um individuo ou de uma organização e validação das solicitações de emissão e revogação de certificados nas Autoridades de Registro.
Agentes Causadores de Eventos	É uma pessoa, organização, dispositivo ou aplicação que causa um evento registrado pelo conjunto de sistemas de auditoria.
Algoritmo	Série de etapas utilizadas para completar uma tarefa, procedimento ou fórmula na solução de um problema. Usado como "chaves" para criptografia de dados.
Algoritmo Assimétrico	É um algoritmo de criptografia que usa duas chaves: uma chave pública e uma chave privada, onde a chave pública pode ser distribuída abertamente enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave.

PALAVRA CHAVE	DESCRIÇÃO
Algoritmo Criptográfico	Processo matemático especificamente definido para cifrar e decifrar mensagens e informações, normalmente com a utilização de chaves.
Algoritmo Simétrico	Algoritmo de criptografia que usa somente uma chave, tanto para cifrar como para decifrar. Esta chave deve ser mantida secreta para garantir a confidencialidade da mensagem. Também conhecido como algoritmo de chave secreta.
Alvará	Documento eletrônico assinado digitalmente pela Entidade Auditora para uma Autoridade de Carimbo do Tempo, através de um sistema de auditoria e sincronismo. Consiste em um certificado de atributo no qual estarão expressos os dados referentes ao sincronismo e o parecer do auditor sobre a exatidão do relógio da entidade auditada.
Ambiente Físico	É aquele composto por todo ativo permanente das entidades integrantes da ICP-Brasil.
Ambiente Lógico	É aquele composto por todo ativo de informação das entidades integrantes da ICP-Brasil.
Análise de Risco	Identificação e avaliação dos riscos (vulnerabilidades e impactos) a que os ativos da informação estão sujeitos.
Aplicações do Certificado	Os certificados da ICP-Brasil são utilizados, de acordo com o seu tipo, em aplicações como: i. **Tipo A**: confirmação da identidade na *web*, correio eletrônico, transações *on-line*, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações. ii. **tipo S**: cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.
Applet	*Applet* é um software aplicativo que é executado no contexto de outro programa.
Arquivo dedicado *(Dedicated File – DF)*	Um DF corresponde a um arquivo que contém informações de controle sobre outros arquivos e, opcionalmente, sobre a memória disponível para alocação. Um DF também pode corresponder a um diretório que permite que outros arquivos e/ou diretórios (EF e DF) possam estar contidos, vinculados ou agrupados [ISO/IEC 7816-4].
Arquivo elementar *(Elementary File – EF)*	Um EF corresponde a um conjunto de unidades de dados ou registros que compartilham o mesmo identificador de arquivo. Por exemplo, dados necessários para uma aplicação são armazenados em EF. Um EF não pode ser "pai" (pertencer a um nível hierárquico superior na árvore de arquivos e diretórios) de outro arquivo [ISO/IEC 7816-4].
Arquivo "Pai"	Corresponde ao arquivo dedicado (DF) imediatamente precedente a um dado arquivo dentro da hierarquia [ISO/IEC 7816-4].
Arquivamento de Chave	É o armazenamento da chave privada para seu uso futuro, após o período de

PALAVRA CHAVE	DESCRIÇÃO
privada	validade do certificado correspondente. Só se aplica a chaves privadas de certificados de sigilo. As chaves privadas de assinatura digital só poderão ser utilizadas durante o período de validade dos respectivos certificados, sendo portanto proibido seu armazenamento.
Arquivamento de chave Pública	É o armazenamento da chave pública, por um período mínimo de 30 anos, para uso futuro, após o período de validade do certificado correspondente com o objetivo de verificar as assinaturas geradas durante o prazo de validade dos respectivos certificados. Só se aplica a chaves públicas de certificados de assinatura. As chaves publicas de sigilo só poderão ser utilizadas durante o período de validade dos respectivos certificados, sendo portanto proibido seu armazenamento.
ASN.1	*Abstract Syntax Notation 1* é uma notação formal usada para descrever os dados transmitidos por protocolos de telecomunicações, não obstante a representação física destes dados, o que quer que a aplicação faça, seja complexo ou muito simples.
Assinatura Digital	Código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um *e-mail* ou uma transação). A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente.
Ataque	i. Ato de tentar desviar dos controles de segurança de um programa, sistema ou rede de computadores. Um ataque pode ser ativo, tendo por resultado a alteração dos dados; ou passivo, tendo por resultado a liberação dos dados. ii. Tentativa de criptoanálise. O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contra-medidas existentes.
Ativação de Chave	Método pelo qual a chave criptográfica fica pronta para exercer suas funções. A ativação da chave se dá por meio de um módulo criptográfico, após a identificação dos operadores responsáveis. A identificação pode ocorrer através de uma senha ou outro dispositivo de controle de acesso como um *token, smart card*, biometria.
Ativo de Informação	É o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos de uma organização.
Ativo de Processamento	É patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos

PALAVRA CHAVE	DESCRIÇÃO
Atribuição de Chaves *(Key Establishment)*	Processo ou protocolo que possibilita atribuir uma chave criptográfica simétrica compartilhada a parceiros legítimos A atribuição de chaves pode ser realizada por um processo automático (protocolo de negociação de chaves ou protocolo de transporte de chaves), método manual ou uma combinação dos anteriores.
Auditor	Profissional que realiza a avaliação dos controles e processos das entidades auditadas. Deve ser idôneo, dotado de capacidades e conhecimentos técnicos específicos e realizar o seu trabalho com observância de princípios, métodos e técnicas geralmente aceitos. Não deve possuir nenhum dos impedimentos ou suspeições estabelecidos nas normas da ICP-Brasil e no Código de Processo Civil.
Auditor Independente	É aquele auditor que não está vinculado aos quadros do ITI nem da entidade auditada. Trabalha para uma empresa de auditoria independente.
Auditoria	Procedimento utilizado para verificar se todos os controles, equipamentos e dispositivos estão preparados e são adequados às regras, normas, objetivos e funções. Inclui o registro e análise de todas as atividades importantes para detectar vulnerabilidades, determinar se houve violação ou abusos em um sistema de informações com vista a possibilitar ao auditor formar uma opinião e emitir um parecer sobre a matéria analisada.
Auditoria de Conformidade	Avaliação da adequação dos processos, procedimentos e atividades das unidades auditadas com a legislação e os regulamentos aplicáveis. Verificam-se todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.
Auditoria Independente	Auditoria realizada por Empresa de Auditoria Especializada e Independente.
Auditoria Operacional	Auditoria de conformidade realizada após o processo de credenciamento. Realizada anualmente ou a qualquer momento, se houver suspeitas de irregularidades.
Auditoria Pré-operacional	Auditoria de conformidade realizada antes do processo de credenciamento.
Autenticação	Processo de confirmação da identidade de uma pessoa física (Autenticação de um Individuo) ou jurídica (Autenticação da Identidade de uma Organização) através das documentações apresentadas pelo solicitante e da confirmação dos dados da solicitação. Executado por Agentes de Registro, como parte do processo de aprovação de uma solicitação de certificado digital.
Autenticação do Agente de Registro	Verificação da identidade de um Agente de Registro, em um sistema computadorizado, como um pré-requisito para permitir o acesso aos recursos de um sistema. Na ICP-Brasil a autenticação do Agente deve se dar com o uso de certificado que tenha requisito de segurança, no mínimo, equivalente ao de um certificado A3.
Autenticação e Sincronização de	Atividade periodicamente realizada pela EAT que resulta na habilitação ou não de um SAS ou de um SCT para operar sincronizado com a Hora Legal

PALAVRA CHAVE	DESCRIÇÃO
Relógio (ASR)	Brasileira. Essas operações devem ser efetuadas por intermédio de um conjunto de protocolos que garantam que o resultado final seja isento de fraudes.
Autenticidade	Qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia e que é livre de adulterações ou qualquer outro tipo de corrupção.
Auto-assinatura digital	É a assinatura feita usando a chave privada correspondente à chave pública associada ao certificado digital.
Auto-teste	A estratégia de auto-teste foi proposta inicialmente para ser utilizada em classes de sistemas orientados a objetos. Nesta estratégia, é incorporada uma especificação de testes à classe, além do acréscimo de funções BIT (do inglês *Built-in Test*) que criam capacidades de observação e controle do estado da classe. A idéia principal é a incorporação ao componente da capacidade de gerar casos de testes automaticamente, ou da inclusão de casos de teste já prontos. Esses casos de teste podem ser executados pelo cliente ou pelo próprio componente.
Autoridade Certificadora (AC)	É a entidade subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). 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). Na hierarquia dos Serviços de Certificação Pública, as AC estão subordinadas à Autoridade Certificadora de nível hierarquicamente superior.
Autoridade Certificadora Raiz (AC Raiz)	Primeira AC da cadeia de certificação da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) cujo certificado é auto-assinado, podendo ser verificado através de mecanismos e procedimentos específicos, sem vínculos com este. Executora das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Compete-lhe emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu; gerenciar a lista de certificados emitidos, revogados e vencidos e executar atividades de fiscalização e auditoria das AC, das AR e dos PSS habilitados na ICP-Brasil, em conformidade com as diretrizes e normas técnicas estabelecidas pelo CG da ICP-Brasil e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.
Autoridade de Carimbo de Tempo (ACT)	A autoridade na qual os usuários de serviços de carimbo do tempo (isto é, os subscritores e as terceiras partes) confiam para emitir carimbos do tempo.
Autoridade de Registro (AR)	Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento,

PALAVRA CHAVE	DESCRIÇÃO
	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.
Autoridade Gestora de Políticas da ICP-Brasil	Vide Comitê Gestor da ICP-Brasil
Autorização	Concessão de direito ou permissão que inclui a capacidade de acessar informações e recursos específicos em um sistema computacional ou permissão de acesso a ambientes físicos.
Autorização de Auditoria Independente	Constitui ato declaratório do Diretor de Auditoria, Fiscalização e Normalização do ITI que permite ao Auditor Independente prestar serviços de auditoria, no âmbito da ICP-Brasil, em conformidade com as normas estabelecidas por este Comitê Gestor.
Avaliação de Conformidade	Conjunto de ensaios com o objetivo de verificar se os padrões e especificações técnicas mínimas aplicáveis a um determinado sistema ou equipamento de certificação digital estão atendidos.
Backup	Vide Cópia de Segurança
Banco de dados	Basicamente é um conjunto de informações relacionadas que são reunidas de forma organizada e categorizada, assim como os "arquivos tradicionais em forma de fichas", porém armazenados em meio magnético (disco de computadores) e que são "Gerenciados" por "Sistemas Especializados", ou, os chamados "Sistemas Gerenciadores de Banco de Dados" (ex: *MYSQL, SQL Server, Oracle, DB2, IMS/DLI, ADABAS*, etc.), que permitem armazenagem, atualização e recuperação dessas informações de forma eficiente (fácil, rápida e precisa) independente do volume.
BASE64	É um método para codificação de dados para transferência na internet (*Content Transfer Enconding*).
BER (Basic Encoding Rules)	Regras para codificação de objetos ASN.1 em uma seqüência de *bytes*.
Biometria	Ciência que utiliza propriedades físicas e biológicas únicas e exclusivas para identificar indivíduos. São exemplos de identificação biométrica as impressões digitais, o escaneamento de retina e o reconhecimento de voz.
Bit (Binary digit)	É a menor unidade de informação possível dentro de um computador. Pode assumir os valores de 0 ou 1.
Bloco	Seqüência de bits de comprimento fixo.
Buffer	É uma região de memória temporária utilizada para escrita e leitura de dados. Os dados podem ser originados de dispositivos (ou processos) externos ou internos ao sistema. Os *buffers* podem ser implementados em software (mais usado) ou hardware. Normalmente são utilizados quando existe uma diferença entre a taxa em que os dados são recebidos e a taxa em que eles podem ser

PALAVRA CHAVE	DESCRIÇÃO
	processados, ou no caso em que essas taxas são variáveis.
***Bureau International des Poids et Mesures* (BIPM)**	Organização central do Sistema Internacional de Metrologia localizada na França e responsável pela geração do UTC.
Cache	É um bloco de memória para o armazenamento temporário de dados que possuem uma grande probabilidade de serem utilizados novamente.
Cadastro de Auditoria Independente	Registro cadastral oficial do ITI das empresas de auditoria especializada e independente. Para almejar o cadastro a empresa deverá apresentar ao ITI rol de documentos previstos na resolução 44 do CG da ICP-Brasil. O cadastro terá validade de 5 anos sendo possível renovações.
Cadeia de AC	São as interligações hierárquicas existentes entre as diversas Autoridades Certificadoras participantes da ICP-Brasil.
Cadeia de Certificação	Uma série hierárquica de certificados assinados por sucessivas autoridades certificadoras.
Carimbo de Tempo	Documento eletrônico emitido pela ACT, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado.
Cartão Inteligente	Vide *Smart Card*
Cavalo-de-Tróia	É um programa no qual um código malicioso ou prejudicial está contido dentro de uma programação ou dados aparentemente inofensivos de modo a poder obter o controle e causar danos.
CBC (Cipher Block Chaining)	É um modo de operação de uma cifra de bloco (ver cifra de bloco), em que o texto plano primeiro é submetido a uma operação binária de XOR com o criptograma resultante do bloco anterior. Algum valor conhecido é usado para o primeiro bloco (normalmente chamado de vetor de inicialização**,** esse valor deve ser único para cada mensagem, mas não precisa ser secreto – pode ser enviado junto com o criptograma, para permitir a decifração). O resultado é então cifrado usando a chave simétrica. Assim, blocos de entrada idênticos em texto claro irão produzir criptogramas diferentes.
Certificação de Data e Hora	Vide *Time-stamping*
Certificação Digital	É a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.
Certificado de Atributo	Estrutura de dados contendo um conjunto de atributos (características e informações) sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Pode possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos.
Certificado Auto-	Certificado assinado com a chave privada da própria entidade que o gerou. O

PALAVRA CHAVE	DESCRIÇÃO
assinado	único certificado auto-assinado da ICP-Brasil é o da Autoridade Certificadora Raiz.
Certificado de Calibração	Documento emitido pelo Observatório Nacional atestando que o equipamento usado para emitir carimbos de tempo (SCT) está dentro dos padrões de sincronismo esperados e está apto a entrar em funcionamento.
Certificado de Assinatura Digital (A1, A2, A3 e A4)	São os certificados usados para confirmação da identidade na *web*, correio eletrônico, transações *on-line,* redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações.
Certificado de Especificações	Documento com as descrições dos requisitos atendidos pelo SCT, no qual o seu fabricante declara responsabilidade sobre estas características. Cada certificado é restrito a um SCT.
Certificado de Sigilo (S1, S2, S3 e S4)	São os certificados usados para cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.
Certificado digital	É um conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.
Certificado do Tipo A1 e S1	É o certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha, cifrado por *software.* Sua validade máxima é de um ano, sendo a freqüência de publicação da LCR no máximo de 48 horas e o prazo máximo admitido para conclusão do processo de revogação de 72 horas.
Certificado do Tipo A2 e S2	É o certificado em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em Cartão Inteligente ou *Token,* ambos sem capacidade de geração de chave e protegidos por senha. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de dois anos, sendo a freqüência de publicação da LCR no máximo de 36 horas e o prazo máximo admitido para conclusão do processo de revogação de 54 horas.
Certificado do Tipo A3 e S3	É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou *Token*, ambos com capacidade de geração de chaves e protegidos por senha, ou *hardware* criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de três anos, sendo a freqüência de publicação da LCR no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação de 36 horas.
Certificado do Tipo A4 e S4	É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou *Token*, ambos com capacidade de geração de chaves e protegidos por senha, ou *hardware* criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 2048 bits. A validade máxima do certificado é de três anos, sendo a freqüência

PALAVRA CHAVE	DESCRIÇÃO
	de publicação da LCR no máximo de 12 horas e o prazo máximo admitido para conclusão do processo de revogação de 18 horas.
Certificado Expirado	Certificado cuja data de validade foi ultrapassada.
Certificado Válido	É um certificado que está dentro do prazo de validade, não tendo sido revogado e sendo possível validar toda a cadeia do certificado até uma AC Raiz aceita pelo usuário que recebe e valida o certificado.
CFB (Ciphertext Feedback)	É um modo de operação para uma cifra de bloco (ver Cifra de Bloco), no qual a saída do sistema é retro-alimentada no mecanismo. Depois que cada bloco é cifrado, parte dele sofre um deslocamento em um registrador. O conteúdo desse registrador é cifrado usando a chave do usuário e a saída sofre uma nova operação binária de XOR com os dados de entrada, para produzir o criptograma. Nesse modo, podemos trabalhar com blocos de mensagens menores do que o tamanho nativo do algoritmo. Dependendo do sistema externo onde está inserido o sistema criptográfico, isso pode trazer vantagens, pois evita a utilização de *buffers* para armazenar temporariamente elementos da mensagem até completar o tamanho de bloco do algoritmo. Efetivamente, o que se irá obter é uma conversão do algoritmo, que opera em forma nativa como cifrador de blocos, em um sistema de cifração seqüencial. Esse método é auto-sincronizável e permite que o usuário decifre apenas uma parte de uma grande base de dados, se começar a partir de uma distância fixa dos dados desejados.
Chave Criptográfica	É o valor numérico ou código usado com um algoritmo criptográfico para transformar, validar, autenticar, cifrar e decifrar dados.
Chave Criptográfica em Texto Claro	Representa uma chave criptográfica não cifrada.
Chave Criptográfica Secreta	Vide Chave Privada e Chave Simétrica
Chave de Sessão	Chave para sistemas criptográficos simétricos. Utilizada pela duração de uma mensagem ou sessão de comunicação. O protocolo SSL (*Secure Sockets Layer)* utiliza as chaves de sessão para manter a segurança das comunicações via internet.
Chave Privada	Uma das chave de um par de chaves criptográficas (a outra é uma chave pública) em um sistema de criptografia assimétrica. É mantida secreta pelo seu dono (detentor de um certificado digital) e usada para criar assinaturas digitais e para decifrar mensagens ou arquivos cifrados com a chave pública correspondente.
Chave Pública	Uma das chaves de um par de chaves criptográficas (a outra é uma chave privada) em um sistema de criptografia assimétrica. É divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente. Dependendo do algoritmo, a chave pública também é usada para cifrar mensagens ou arquivos que possam, então, ser decifrados com a chave privada correspondente.

PALAVRA CHAVE	DESCRIÇÃO
Chave Simétrica	Chave criptográfica gerada por um algoritmo simétrico (Ver Algoritmo Simétrico).
Chaves Assimétricas	Chaves criptográficas geradas por um algoritmo assimétrico (Ver Algoritmo Assimétrico).
Ciclo de Vida do Certificado	Período de tempo que se inicia com a solicitação do certificado e termina com sua expiração ou revogação.
Cifra de Bloco	Algoritmo criptográfico simétrico, no qual a mensagem é dividida em blocos e cada bloco é cifrado separadamente.
Cifrar	i. É o processo de transformação de dados ou informação para uma forma ininteligível usando um algoritmo criptográfico e uma chave criptográfica. Os dados não podem ser recuperados sem usar o processo inverso de decifração. ii. Processo de conversação de dados em "código ilegível" de forma a impedir que pessoas não autorizadas tenham acesso à informação.
Classificação da Informação	Ato ou efeito de analisar e identificar o conteúdo de documentos, atribuindo um grau de sigilo que define as condições de acesso aos mesmos, conforme normas e legislação em vigor.
CMM-SEI (Capability Maturity Model do Software Engineering Institute)	Modelo para avaliação da maturidade dos processos de software de uma organização e para identificação das práticas-chave que são requeridas para aumentar a maturidade desses processos. O CMM prevê cinco níveis de maturidade: inicial, repetível, definido, gerenciado e otimizado. O modelo foi proposto por Watts S. Humphrey, a partir das propostas de Philip B. Crosby, e vem sendo aperfeiçoado pelo *Software Engineering Institute* - SEI da Carnegie Mellon University.
CMPV (Cryptographic Module Validation Program)	Programa de testes para módulos criptográficos criado pelo *NIST (National Institute of Standards and Technology*, do governo dos Estados Unidos, e pelo CSE (*Communications Security Establishment*) do governo do Canadá, em 1995. Utiliza-se de laboratórios independentes credenciados. Fabricantes interessados nos testes de validação podem selecionar qualquer um dos laboratórios credenciados. Para as validações, são utilizados os requisitos definidos no padrão FIPS 140-2.
CN (Common Name)	Atributo especificado dentro do campo Assunto - Nome Distinto (*Distinguished Name*) - de um certificado. Por exemplo, para certificados de servidor o nome do *"host"* DNS do site a ser certificado; para um Certificado de Assinatura de Software, o nome comum é o nome da organização e em certificados de assinante, o nome comum é normalmente composto pelo prenome e sobrenome do titular.
Co-assinatura	A co-assinatura (*co-sign)* é aquela gerada independente das outras assinaturas.
Código de Autenticação	Corresponde a um verificador criptográfico de integridade e autenticidade que é comumente referenciado como MAC (*Message Authentication Code*).

PALAVRA CHAVE	DESCRIÇÃO
Comitê Gestor da ICP-Brasil	Autoridade gestora de políticas da ICP-Brasil que tem suas competências definidas na Medida Provisória 2.200-2. É responsável, dentre outras coisas, por estabelecer a política e as normas de certificação, fiscaliza a atuação da Autoridade Certificadora Raiz, cuja atividade é exercida pelo Instituto Nacional de Tecnologia da Informação.
Commom Criteria (CC)	É um padrão internacional (ISO/IEC 15408) para a segurança do computador. CC fornece a garantia que o processo da especificação, da execução e da avaliação de um produto de segurança do computador foi conduzido de modo rigoroso e padronizado.
Compensação (*Offset*)	Correção necessária no relógio local para fazer com que indique o mesmo tempo indicado pelo relógio de referência.
Comprometimento	Violação concreta ou suspeita de violação de uma política de segurança de um sistema, onde possa ter ocorrido divulgação não autorizada ou perda do controle sobre informações sigilosas.
Confiança	É a suposição de que uma entidade se comportará substancialmente como esperado no desempenho de uma função específica.
Confidencial	Tipo de classificação de informação, que se for divulgada ou usada sem autorização, trará sérios prejuízos para uma organização.
Confidencialidade	Propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. Assegurar a confidencialidade de documentos é assegurar que apenas pessoas autorizadas tenham acesso à informação.
Confirmação da Identidade	Vide Autenticação da Identidade
Consulta *On-line* de Situação do Certificado	Vide OCSP
Conta	Permissão para acesso a um serviço. A permissão é obtida após o registro de dados específicos do usuário, no servidor, que definem o ambiente de trabalho desse usuário. O registro pode incluir configurações de tela, configurações de aplicativos e conexões de rede. O que o usuário vê na tela, além de quais arquivos, aplicativos e diretórios ele tem acesso é determinado pela maneira com que foi configurada a conta do usuário.
Contexto Seguro de Execução	Estrutura de dados existente durante a execução da biblioteca criptográfica onde as chaves criptográficas estão protegidas contra divulgação, modificação e substituição não autorizada.
Contingência	Situação excepcional decorrente de um desastre.
Contra-assinatura	A contra-assinatura (*countersign*) é aquela realizada sobre uma assinatura já existente. Na especificação CMS a contra-assinatura é adicionada na forma de um atributo não autenticado (*countersignature attribute*) no bloco de informações (*signerInfo)* relacionado à assinatura já existente.

PALAVRA CHAVE	DESCRIÇÃO
Controle “n de m”	Forma de controle múltiplo onde “n” pessoas de um grupo de “m”, são requeridas para utilização de uma chave privada.
Controle de Acesso	i. Conjunto de componentes dedicados a proteger a rede, aplicações *Web* e instalações físicas de uma AC contra o acesso não autorizado, permitindo que somente organizações ou indivíduos previamente identificados e autorizados possam utilizá-las. ii. Restrições ao acesso às informações de um sistema, exercidas pela gerência de segurança da entidade detentora daquele sistema.
Controles	i. Procedimentos usados para controlar o sistema de tal maneira que ele esteja de acordo com critérios especificados. ii. Qualquer ação, procedimento, técnica ou qualquer outra medida que reduza a vulnerabilidade de uma ameaça a um sistema.
Cópia de Segurança	São as cópias feitas de um arquivo ou de um documento que deverão ser guardadas sob condições especiais para a preservação de sua integridade no que diz respeito tanto à forma quanto ao conteúdo, de maneira a permitir o resgate de programas ou informações importantes em caso de falha ou perda dos originais.
COTEC	O Comitê Técnico - COTEC - presta suporte técnico e assistência ao Comitê Gestor da ICP-Brasil, sendo responsável por manifestar previamente sobre as matérias apreciadas e decididas pelo comitê Gestor.
Credenciamento	Entende-se como o processo em que o ITI avalia e aprova os documentos legais, técnicos, as práticas e os procedimentos das entidades que desejam ingressar na ICP-Brasil. Aplica-se a Autoridades Certificadoras, Autoridades de Registro e Prestadores de Serviços de Suporte. Quando aprovados, os credenciamentos são publicados no Diário Oficial da União.
CryptoAPI	*Cryptographic Application Programming Interface* (também conhecida como *CryptoAPI, Microsoft Cryptography API*, ou simplesmente *CAPI*) é uma interface de programação para aplicações incluída com o sistema operacional *Microsoft Windows* que provê serviços para habilitar desenvolvedores para aplicações de segurança baseadas em *Windows* usando criptografia. É um conjunto de bibliotecas dinamicamente ligadas que provê um nível de abstração que isola programadores do código usado para cifrar dados.
Criptografar	Ver Cifrar
Criptografia	i. Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo, impedir modificações, uso não autorizado e dar segurança à confidência e autenticação de dados. ii. Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem. A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito à formas de recuperar aquela informação sem se ter os parâmetros completos para a decifragem.

PALAVRA CHAVE	DESCRIÇÃO
Criptografia Assimétrica	É um tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.
Criptografia de Chaves Públicas	Ver Criptografia Assimétrica
CSP (Cryptographic Service Provider)	É uma biblioteca de software que implementa a *Cryptographic Application Programming Interface (CAPI)*. CSP's implementam funções de codificação e decodificação, que os programas de aplicação de computador podem usar para, por exemplo, autenticação segura de usuário ou para o email seguro. CSP's são executados basicamente como um tipo especial de DLL com limitações especiais no carregamento e no uso.
Curvas Elípticas	A criptografia de curvas elípticas (ECC) é uma abordagem de criptografia de chave pública baseada na estrutura algébrica de curvas algébricas de campos finitos. As curvas elípticas são usadas também em diversos algoritmos do fatoração de inteiro que tem aplicações em criptografia.
Custódia	Consiste na responsabilidade jurídica de guarda e proteção de um ativo, independente de vínculo de propriedade. A custódia, entretanto, não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.
Dados	Informações representadas em forma digital, incluindo voz, texto, *fac-símile*, imagens e vídeo.
Dados de Ativação	Valores de dados, que não sejam chaves criptográficas, necessários para operar módulos criptográficos e que necessitam ser protegidos (ex.: PIN, *passphrase* ou uma chave compartilhada manualmente).
Data de validade do Certificado	A hora e a data de quando termina o período operacional de um certificado digital. Não tem relação com a revogação antes da hora e data anteriormente prevista.
Datação de Registros	É o serviço de certificação da hora e do dia em que foi assinado um documento eletrônico, com identidade do autor.
Decifrar	Processo que transforma dados previamente cifrados e ininteligíveis de volta à sua forma legível.
Declaração das Práticas de Carimbo de Tempo (DPCT)	Declaração das práticas e dos procedimentos empregados pela ACT para emitir Carimbos do Tempo.
Declaração de Praticas de Certificação (DPC)	Documento, periodicamente revisado e republicado, que descreve as práticas e os procedimentos empregados pela Autoridade Certificadora na execução de seus serviços. É a declaração a respeito dos detalhes do sistema de credenciamento, as práticas, atividades e políticas que fundamentam a emissão de certificados e outros serviços relacionados. É utilizado pelas

PALAVRA CHAVE	DESCRIÇÃO
	Autoridades Certificadoras para garantir a emissão correta dos certificados e pelos solicitantes e partes confiantes para avaliar a adequação dos padrões de segurança empregados às necessidades de segurança de suas aplicações.
Decriptografar	Ver Decifrar
DER (Distinguished Encoding Rules)	Regras para codificação de objetos ASN.1 em uma seqüência de *bytes*. Corresponde a um caso especial de BER.
DES (Data Encryption Standard)	Algoritmo simétrico de criptografia de dados que utiliza um sistema de cifragem em blocos. Foi criado pela IBM em 1977 e apesar de permitir cerca de 72 quadrilhões de combinações (2^{56}), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na internet. Está definido no documento de padronização FIPS 46-1.
Desastre	i. É um evento súbito e inesperado cujo impacto resulta em perdas significativas para a organização. ii. Uma circunstância em que um negócio é julgado incapaz de funcionar em conseqüência de alguma ocorrência natural ou criada.
Desativação de Chave	Contrário de ativação de chave (ver Ativação de Chave).
Destruição de Chave	Refere-se à destruição física da mídia armazenadora e/ou lógica (sobrescrever os espaços onde a chave estiver armazenada) da chave criptográfica.
Diffie-Hellman	*Diffie-Hellman* é um método de criptografia desenvolvido por Whitfield Diffie e Martin Hellman e publicado em 1976. O algoritmo *Diffie-Hellman* permite que haja a troca de chaves públicas entre duas ou mais partes, permitindo que as pessoas que recebem a chave pública usem essa chave para cifrar o conteúdo de uma mensagem que será enviada à parte que forneceu a chave pública. Esse texto cifrado não poderá ser aberto por indivíduos que possuam a chave pública e sim, apenas pela parte que enviou a chave pública, pois a mesma possui a chave privada que se encontra em seu poder. Tendo posse dessa chave a mensagem cifrada poderá ser aberta.
Direito de Acesso	É o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.
Diretório	Unidade lógica de armazenamento que permite agrupar arquivos em pastas hierárquicas e subpastas.
Disponibilidade	É a razão entre o tempo durante o qual o sistema está acessível e operacional e o tempo decorrido. No âmbito da ICP-Brasil a disponibilidade das informações publicadas pelas AC em serviço de diretório ou página *web* deve ser de 99% do mês, 24 horas por dia e 7 dias por semana.
DMZ (Demilitarized Zone)	Uma área na rede de uma empresa que é acessível à rede pública (internet), mas não faz parte da sua rede interna. Geralmente, esses servidores possuem números de IP acessíveis pela rede externa, o que os torna alvos de ataques. Para assegurar que os riscos são minimizados, um sistema de detecção e

PALAVRA CHAVE	DESCRIÇÃO
	prevenção de intrusos deve ser implementado nessa DMZ.
DN (Distinguished Name)	Conjunto de dados que identifica de modo inequívoco uma entidade ou indivíduo pertencente ao mundo físico no mundo digital (por exemplo: país=BR, estado=Rio de Janeiro, nome organizacional=Sua Empresa S.A., nome comum=José da Silva).
DNS (Domain Name Service)	É um serviço e protocolo da família TCP/IP para o armazenamento e consulta às informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes internet em seus números IP correspondentes.
Documentação técnica	Conjunto de documentos técnicos que acompanham o objeto de homologação e que a parte interessada deve depositar no LSITEC-LEA para servir ao processo de homologação. A documentação técnica deve apresentar uma descrição técnica sobre o objeto de homologação que satisfaça aos requisitos definidos no MCT.
Documento	Unidade de registro de informações, qualquer que seja o suporte.
Documento digital	Unidade de registro de informações, codificada por meio de dígitos binários.
Documento Eletrônico	Unidade de registro de informações, acessível por meio de um equipamento eletrônico.
Drift	Variação no *skew* (segunda derivada do *offset*) apresentada por alguns relógios.
DSA (Digital Signature Algarithm)	Algoritmo unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão DSS (*Digital Signature Standard)*. Adotado como padrão final em dezembro de 1994, trata de uma variação dos algoritmos de assinatura ElGamal e Schnorr. Foi inventado pela NSA e patenteado pelo governo americano.
ECB (Electronic Code Book)	É um modo de operação de uma cifra de bloco (ver cifra de bloco), com a característica que cada bloco possível de “texto claro” tem um valor correspondente definido da mensagem cifrada e vice-versa. Ou seja o mesmo valor de “texto claro” resultará sempre no mesmo valor da mensagem cifrada. ECB é usado quando um volume de “texto claro” é dividido em diversos blocos dos dados, onde cada um é então cifrado independentemente de outros blocos. De fato, ECB tem a capacidade de suportar uma chave separada de cifração para cada tipo do bloco.
e-PING	Padrões de Interoperabilidade de Governo Eletrônico: define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de Serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais poderes e esferas de governo e com a sociedade em geral. As áreas cobertas pela e-PING, estão segmentadas em: " Interconexão; " Segurança; " Meios de Acesso; " Organização e Intercâmbio de Informações; " Áreas e Assuntos de Integração para Governo Eletrônico.
Elemento de Dado	No contexto da norma ISO/IEC 7816-4 referente ao cartão inteligente, um

PALAVRA CHAVE	DESCRIÇÃO
	elemento de dado corresponde a um item de informação para o qual é associado um nome, uma descrição de conteúdo lógico, um formato e uma codificação [ISO/IEC 7816-4].
Emitir Certificado Digital	É a atividade de geração de um Certificado Digital, a inclusão neste dos dados de identificação do seu emissor (Autoridade Certificadora), do titular e da sua assinatura digital e subseqüente notificação ao seu solicitante, observados os dispostos nos documentos públicos das AC denominados Práticas de Certificação - PC e Declaração de Práticas de Certificação – DPC.
Empresa de Auditoria Especializada e Independente	Vide Empresa de Auditoria Independente
Empresa de Auditoria Independente	São empresas de Auditoria Independentes, autorizadas pelo ITI para atuar na ICP-Brasil e que podem ser contratadas pelas autoridades certificadoras para realizar auditorias operacionais em entidades a elas subordinadas.
Encadeamento	Ato de associar um carimbo de tempo a outro.
Encriptar	Ver Cifrar
Engenharia Social	É o termo utilizado para a obtenção de informações importantes de uma organização, através de seus usuários e colaboradores, ou de uma pessoa física. Essas informações podem ser obtidas pela ingenuidade ou confiança. Os ataques desta natureza podem ser realizados através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e até mesmo pessoalmente.
Ensaio	Procedimento técnico realizado em conformidade com as normas aplicáveis, que objetiva analisar um ou mais requisitos técnicos de um dado sistema ou equipamento.
Entidade de Auditoria de Tempo (EAT)	Entidade que realiza as atividades de autenticação e sincronismo de Servidores de Carimbo do Tempo (SCT), instalados nas ACT. Na estrutura de carimbo do tempo da ICP-Brasil, a EAT é o próprio Observatório Nacional.
Entidades Operacionalmente Vinculadas	Entidade relacionada a outra: i. como matriz, subsidiária, sócia, *joint-venture,* contratada ou agente, ii. como membro de uma comunidade de interesses registrada, ou iii. como entidade que mantém relacionamento com uma entidade principal, que mantém negócios ou registros capazes de fornecer comprovação adequada da identidade da afiliada. No caso da ICP-Brasil, diz-se que uma AR ou PSS está operacionalmente vinculada a uma AC, por exemplo.
Entidade Usuária Externa	Um indivíduo ou processo que realiza acesso a um módulo criptográfico independentemente do papel assumido.
Enveloped Data	Consiste em conteúdo cifrado de todos os tipos e chaves cifradas de sessão do tipo *"content-encryption"* para um ou mais recipientes. As mensagens *"enveloped"* mantêm os conteúdos do segredo da mensagem e reservam-nos

PALAVRA CHAVE	DESCRIÇÃO
	somente a pessoas ou entidades para recuperar os conteúdos. *Cryptographic message syntax (CMS)* pode ser usado para codificar mensagens *"enveloped".*
Equipamento de Certificação Digital	Todo e qualquer aparelho, dispositivo ou elemento físico que compõe meio necessário ou suficiente à realização de Certificação Digital
Erro	Diferença de tempo medida pelo Observatório Nacional entre o SAS e o SCT da ACT.
Erro Máximo Acumulado	Erro máximo que pode ser acumulado pelo relógio interno do SCT, entre duas ASR.
Estabilidade	Capacidade de um oscilador em manter a mesma freqüência em um determinado intervalo de tempo.
***Escrow* de Chave Privada**	Vide Recuperação de Chave
Evento	São ocorrências de significância, eletrônicas ou manuais, que devem ser registradas para análises e auditorias posteriores. Na ICP-Brasil, há diversos tipos de eventos que devem obrigatoriamente ser registrados, como: iniciação e desligamento do sistema de certificação; tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC etc.
Exatidão	Afastamento máximo tolerado entre o valor indicado por um sistema de medição e o valor verdadeiro do tempo.
Expoente Privado	Representa o expoente na definição de chave privada: par (d, n) onde "d" é o expoente privado e "n" é o módulo público (produto de dois fatores primos privados).
Expoente Público	Representa o expoente na definição de chave pública: par (e, n) onde "e" é o expoente público e "n" é o módulo público (produto de dois fatores primos privados).
Exportação de certificado digital	É a atividade de copiar um Certificado Digital instalado em determinado computador ou hardware, para um disquete, CD, etc, permitindo a sua instalação em outro(s) computador(es) ou hardware.
Exportação de chaves criptográficas	Processo de retirada de chave criptográfica do módulo criptográfico. A exportação pode ser realizada de forma manual ou automática.
Exportação de chaves criptográficas de forma automática	Processo de retirada de chave criptográfica de um módulo criptográfico que utiliza uma mídia eletrônica ou meio de comunicação eletrônico.
Exportação de chaves criptográficas de forma manual	Processo de retirada de chave criptográfica do módulo criptográfico que utiliza métodos manuais. Ex: apresentação do valor da chave um *display.*
***FIPS (Federal Information Processing Standards*)**	Correspondem aos padrões e diretrizes desenvolvidos e publicados pelo NIST (*National Institute of Standards and Technology*) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST

PALAVRA CHAVE	DESCRIÇÃO
	desenvolve os padrões e diretrizes FIPS quando há requisitos obrigatórios do governo federal, tais como, segurança e interoperabilidade e não há padrões ou soluções industriais aceitáveis.
FIPS 140 Federal Information Processing Standards)	O *Federal Information Processing Standards* 140 é um padrão do governo dos Estados Unidos para implementações de módulos de criptografia - ou seja, hardware e software para cifrar e decifrar dados ou realizar outras operações criptográficas (como geração ou verificação de assinaturas digitais). Encontra-se atualmente na versão 2, estando em elaboração, pelo NIST, a versão 3.
Firewall	É um conjunto formado por Hardware, Software e uma política de acesso instalado entre redes, com o propósito de segurança. A função do *firewal*l é controlar o tráfego entre duas ou mais redes, com o objetivo de fornecer segurança, prevenir ou reduzir ataques ou invasões às bases de dados corporativas, a uma (ou algumas) das redes, que normalmente têm informações e recursos que não devem estar disponíveis aos usuários da(s) outra(s) rede(s).
Firmware	Programas e componentes de dados de um módulo que estão armazenados em uma porção de hardware (ROM, PROM, EPROM, EEPROM ou FLASH, por exemplo) que não podem ser dinamicamente escritos ou modificados durante a execução.
Fonte Confiável de Tempo (FCT)	É a denominação dada ao Relógio Atômico localizado no Observatório Nacional.
Fronteira criptográfica (*Cryptographic Boundary*)	A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico.
Geração de Par de Chaves	Processo de criação de um par de chaves (chave privada e chave pública), sendo normalmente executado na solicitação de um certificado digital.
Gerador de Números Aleatórios	Vide *RNG*
Gerador de Números Pseudo-aleatórios	Vide *PRNG*
Gerenciamento de Certificado	É a forma como uma AC, baseada em suas DPC, PC e PS, atua na emissão, renovação e revogação de certificados, bem como na emissão e publicação da sua LCR.
Gerenciamento de Risco	Processo que visa a proteção dos ativos das entidades integrantes da ICP-Brasil, por meio da eliminação, redução ou transferência dos riscos, conforme seja econômica e estrategicamente mais viável.
Hacker	Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.
Handle	i. Um dispositivo, unido a um objeto, que seja anexado para mover ou usar o

PALAVRA CHAVE	DESCRIÇÃO
	objeto. ii. um tipo do ponteiro inteligente, uma referência a uma posição na memória de computador.
Hardware	i. Conjunto dos componentes físicos necessários à operação de um sistema computacional. ii. Equipamento mecânico e eletrônico, combinado com *software* (programas, instruções, etc.) na implementação de um sistema de processamento de informações eletrônicas.
Hardware Secure Module (HSM)	É um dispositivo baseado em *hardware* que gera, guarda e protege chaves criptográficas, além de ter a capacidade de executar operações criptográficas, como assinatura digital.
Hash	É o resultado da ação de algoritmos que fazem o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor - conhecido como resultado *hash* - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (dado um *hash*, não é possível recuperar a mensagem que o gerou).
Hibernação	Um mode de *"power-saving"* que conserve a bateria do computador, mas permite uma reativação mais rápida da operação do que desligando o computador e então voltando a ligá-lo. Quando o modo de hibernação é ativado, todas as aplicações atuais que estão na memória estão conservadas no disco e o computador é desligado. Ao retomar a operação, pressionando uma tecla ou clicando o *mouse*, as aplicações são lidas do disco e voltam ao mesmo estado anterior.
Hierarquia do Certificado	Uma estrutura de certificados digitais que permite a indivíduos verificarem a validade de um certificado. O certificado é emitido e assinado por uma Autoridade Certificadora que está numa posição superior na hierarquia dos certificados. A validade de um certificado específico é determinada, entre outras coisas, pela validade correspondente ao certificado da AC que fez a assinatura.
Homologação	Processo que consiste no conjunto de atos, realizados de acordo com um Regulamento e com as demais normas editadas ou adotadas pela ICP-Brasil, que, se plenamente atendido, resultará na expedição de ato pelo qual, na forma e nas hipóteses previstas, a entidade responsável pela condução do referido processo reconhecerá o laudo de conformidade.
HSM (Hardware Security Modules)	Vide Módulo de Segurança Criptográfica
IDEA (International Data Encryption Algorithm)	Algoritmo criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas, na maioria dos microprocessadores, uma implementação por soft*w*a*re* do IDEA é mais rápida do que uma implementação por *software* do DES. O IDEA é o programa para criptografia de *e-mail* pessoal mais disseminado no mundo. Seu tamanho de chave é de 128 bits.

PALAVRA CHAVE	DESCRIÇÃO
Identificação	Vide Autenticação
Identificador de Registro	Valor associado a um registro que pode ser usado para referenciar aquele registro. Diversos registros poderiam ter o mesmo identificador dentro de um EF [ISO/IEC 7816-4].
Importação de Certificado Digital	É a atividade de copiar um Certificado Digital a partir de um disquete, CD, *smart card,* para um computador ou hardware, permitindo a sua instalação e uso posterior, por exemplo, para assinatura digital de *e-mails.*
Importação de chaves criptográficas	Processo de inserção de chave criptográfica no módulo criptográfico. A importação pode ser realizada de forma manual ou automática.
Importação de chaves criptográficas de forma automática	Processo de inserção de chave criptográfica de um módulo criptográfico que utiliza uma mídia eletrônica ou meio de comunicação eletrônico.
Importação de chaves criptográficas de forma manual	Processo de inserção de chave criptográfica de um módulo criptográfico que utiliza métodos manuais. Ex: digitação em um teclado, por uma entidade usuária externa, do valor da chave.
Incerteza	Dispersão dos valores que podem ser atribuídos a um mensurando, como resultado de uma sincronização.
Incidente de Segurança	É qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo das entidades integrantes da ICP-Brasil.
Infra-estrutura de chaves públicas brasileira (ICP-Brasil)	É um conjunto de técnicas, arquitetura, organização, práticas e procedimentos, implementados pelas organizações governamentais e privadas brasileiras que suportam, em conjunto, a implementação e a operação de um sistema de certificação. Tem como objetivo estabelecer os fundamentos técnicos e metodológicos de uma sistema de certificação digital baseado em criptografia de chave pública, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. A ICP-Brasil foi criada pela Medida Provisória 2200-2, de 24.08.2001 e está regulamentada pelas Resoluções do Comitê-Gestor da ICP-Brasil, disponíveis no sítio www.iti.gov.br.
Instituto Nacional de Tecnologia da Informação (ITI)	É uma autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz da ICP-Brasil. É a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.
Integridade	Garantia oferecida ao usuário de que documento eletrônico, mensagem ou conjunto de dados não foi alterada, nem intencionalmente, nem acidentalmente por pessoas não autorizadas durante sua transferência entre sistemas ou computadores.
Interface	Representa um ponto lógico de entrada e saída de dados, que provê acesso

PALAVRA CHAVE	DESCRIÇÃO
	aos serviços disponíveis pelos softwares.
Intimação	Ato pelo qual se dá conhecimento do procedimento de fiscalização para que a entidade fiscalizada faça ou deixe de fazer alguma coisa.
Irretratabilidade	Consiste basicamente em um mecanismo para garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a autoria.
ISO (International Standards Organization)	É a organização que cria padrões internacionais para diversas áreas, incluindo computadores. Congrega em torno de 90 países.
ITU (International Telecommunication Union)	É uma organização internacional que faz parte do Sistema das Nações Unidas. Responsável pelo estabelecimento de normas e padrões em telecomunicações e seus serviços.
Key Containers	Uma parte do *key database* (banco de dados que contém as chaves criptográficas para um *CSP* específico) que contém todos os pares de chaves (pares de chaves para troca e assinatura) que pertencem a um usuário específico. Cada recipiente tem um nome único que é usado ao chamar funções de contexto para obter um *handle* ao *container*.
Key Zeroization	Um método de apagar chaves criptográficas armazenadas eletronicamente, alterando ou suprimindo os índices de armazenamento das chaves para impedir a recuperação das informações.
Laboratório de Ensaio e Auditoria (LEA)	São entidades, formalmente vinculadas ao ITI, aptas a realizar os ensaios exigidos nas avaliações de conformidade e a emitir os correspondentes laudos de conformidade, na forma prevista na resolução nº 36 do CG da ICP-Brasil, que embasarão a tomada de decisão por parte do ITI quanto à homologação ou não de um dado sistema ou equipamento avaliado.
Laudo de Conformidade	Documento emitido ao final da avaliação de conformidade, na forma prevista na resolução nº 36 do CG da ICP-Brasil , que atestará se um dado sistema ou equipamento, devidamente identificado, está ou não em conformidade com as normas editadas ou adotadas pela ICP-Brasil.
Leap second	Segundo adicionado ao UTC para compensar o atraso da rotação da Terra e manter o UTC em sincronismo com o tempo solar.
Leitora de Cartão Inteligente	Hardware instalado no computador, utilizando de interface serial ou usb, que serve para efetuar leituras de *smart cards.*
Lista de Certificados Revogados (LCR)	Lista assinada digitalmente por uma Autoridade Certificadora, publicada periodicamente, contendo certificados que foram revogados antes de suas respectivas datas de expiração. A lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.
Lista de Controle de Acesso	Lista de indivíduos ou entidades com permissão de acesso a certas áreas específicas de um servidor, rede, aplicação de internet ou instalações físicas.
Log	Conjunto de registros que lista as atividades realizadas por uma máquina ou

PALAVRA CHAVE	DESCRIÇÃO
	usuário específico. Um único registro é conhecido como 'registro de log'. Em termos de segurança, os *logs* são usados para identificar e investigar as atividades suspeitas e estudar as tentativas (ou os sucessos) dos ataques, para conhecimento dos mecanismos usados e aprimoramento do nível de eficiência da segurança.
Login	É o processo de identificação e autenticação ao qual o usuário é submetido antes de integrar ao sistema, software ou aplicativo.
Logoff	É o processo de encerramento da sessão de trabalho pelo usuário.
MAC (Message Authentication Code)	É uma pequena parte de informação usada para autenticar uma mensagem. Um algoritmo MAC aceita como entrada uma chave secreta e uma mensagem de comprimento indefinido para ser autenticado e envia como saída um MAC (conhecido às vezes como *tag)*. O valor do MAC protege a integridade de uma mensagem assim como sua autenticidade, permitindo que os verificadores (quem possuem também a chave secreta) detectem todas as mudanças no conteúdo da mensagem.
MD5 *(Message Digest 5)*	É uma função de *hash* - espalhamento unidirecional - inventada por Ron Rivest. Este algoritmo produz um valor *hash* de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sido descobertos contra a função *hashing* prévia: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor *hash* de somente 128 bits é o que causa maior preocupação.
Mídia	Base física (*hardware*) ou lógica (*software*) sobre a qual a informação é registrada, podendo ser exportada para outra mídia ou permanecer armazenada nela própria.
Mídia Armazenadora	Vide Mídia.
MIME (Multipurpose Internet Mail Extensions)	É um padrão da internet que estende o formato de *e-mail* para suportar: texto em conjunto de caracteres além do tipo *US-ASCII*; anexos do tipo *não-texto*; corpos de mensagem do tipo *multi-part* e informação de cabeçalho em conjunto de caracteres do tipo *não-ASCII.* Os tipos de conteúdo definidos por padrões MIME são também de importância além do *e-mail*, como em protocolos de comunicação como o HTTP para a internet.
Mitigação	Os esforços da mitigação tentam impedir que perigos se tornem desastres completamente, ou reduzem os efeitos dos desastres quando ocorrem. A mitigação focaliza em medidas a longo prazo para se reduzir ou eliminar riscos. A implementação de estratégias de mitigação pode ser considerada uma parte do processo da recuperação se aplicado após a ocorrência de um desastre.
Módulo Criptográfico	Software ou hardware que fornece serviços criptográficos, como cifração,

PALAVRA CHAVE	DESCRIÇÃO
	decifração, geração de chaves, geração de números aleatórios.
Módulo criptográfico mono-CI	Módulo criptográfico com um único circuito integrado protegido por um invólucro.
Módulo criptográfico multi-CI	Módulo criptográfico com vários circuitos integrados protegidos por um invólucro.
Módulo criptográfico multiaplicação	Faz referência a um módulo criptográfico que suporta mais que uma aplicação. Exemplo: módulo criptográfico contendo aplicação ICP e aplicação EMV.
Módulo de Segurança Criptográfica (MSC)	É um *hardware* com capacidade de processamento, que gera chaves criptográficas e assina documentos, sendo usado para para assinar os certificados digitais em Autoridades Certificadoras, oferecendo grande velocidade e segurança.
Multi-threaded	Característica dos sistemas operativos modernos que permite repartir a utilização do processador entre várias tarefas simultaneamente.
Não-repúdio	Não-Repúdio, ou não recusa, é a garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos de um uso indevido do certificado digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação. Transações digitais estão sujeitas a fraude, quando sistemas de computador são acessados indevidamente ou infectados por cavalos-de-tróia ou vírus. Assim os participantes podem, potencialmente, alegar fraude para repudiar uma transação.
Navegador de internet ou *Browser*	Aplicativo utilizado para visualizar arquivos HTML, VRML, textos, arquivos de áudio, animação, videoclipes e/ou correio eletrônico pela internet. Entre os principais navegadores disponíveis no mercado estão: Microsoft Internet Explorer, Netscape Navigator, Opera, Mozilla, etc.
NBR (Norma Brasileira Regulamentadora)	É a sigla de Norma Brasileira aprovada pela ABNT, de caráter voluntário e fundamentada no consenso de um grupo de representantes da comunidade científica. Suas disposições abrangem diversos temas e são obrigatórias quando em condições estabelecidas pelo poder público competente.
Negociação de chaves (*Key Agreement*)	Processo ou protocolo que possibilita atribuir uma chave criptográfica simétrica compartilhada aos parceiros legítimos em função de valores secretos escolhidos por cada um dos parceiros, de forma que nenhuma outra entidade possa determinar o valor da chave criptográfica. Exemplo clássico de negociação de chaves é o algoritmo *Diffie-Hellman*.
No-breaks	Equipamento que tem como função suprir a energia de um circuito, por um tempo determinado, na ausência da fonte de energia principal da rede elétrica.
Nome Significativo	É aquele que possibilita determinar a identidade da pessoa ou organização a que se refere.
Número de Série do	Um valor que identifica de forma unívoca um certificado emitido por uma

PALAVRA CHAVE	DESCRIÇÃO
Certificado	Autoridade Certificadora.
Número de Identificação Pessoal (*Personal Identification Number* - PIN)	Código alfanumérico ou senha usada para autenticar uma identidade.
Número de Registro	No contexto do sistema de arquivos de cartões inteligentes, representa um número seqüencial atribuído a cada registro, que serve para identificar unicamente o registro dentro de seu EF [ISO/IEC 7816-4].
***Object Identifier* (OID)**	Um OID – *Object Identifier* - é um número único que identifica uma classe de objetos ou um atributo em um diretório ou combinação de diretórios. OIDs são definidos por entidades emissoras e formam uma hierarquia. Um OID é representado por um conjunto de números decimais separados por pontos (ex.: 1.2.3.4). OIDs são usados extensivamente em certificados de formato X.509, como por exemplo, para designar algoritmos criptográficos empregados, políticas de certificação e campos de extensão. Praticamente toda implementação de ICP usando este formato requer o registro de novos OIDs, em particular uma que designe a política de certificação que estabelece seu regime regulatório básico. É crucial que os OIDs sejam obtidos dos legítimos responsáveis pelos arcos, para se evitar incompatibilidades e colisões. Nos certificados da ICP-Brasil os OIDs utilizados para identificar as Políticas de Certificados e Declaração de Práticas de Certificação das Autoridades Certificadoras são atribuídos pelo ITI, durante o processo de auditoria da AC e obedecem a seguinte lógica: **2.16.76.1.1.n –** OID para Declarações de Práticas de Certificação **2.16.76.1.2.n –** OID para Políticas de Certificados **2.16.76.1.3.n e 2.16.76.1.4.n –** OID usados para permitir a inclusão no certificado de outros dados de pessoas físicas e jurídicas, como CNPJ, CPF, título de eleitor, categoria profissional etc.
Objeto de Dado	No contexto do padrão ISO/IEC 7816-4 para cartões inteligentes, um objeto de dado consiste em um conjunto de caracteres (*tag*), um comprimento e um valor (um elemento de dado, por exemplo). Nesta parte do padrão ISO/IEC 7816, objetos de dados são referenciados como BER-TLV, COMPACT-TLV e SIMPLE-TLV [ISO/IEC 7816-4].
Observatório Nacional (ON)	Vinculado ao Ministério da Ciência e Tecnologia, integrante do Sistema Nacional de Metrologia – Sinmetro, o ON é o responsável legal pela geração, conservação e disseminação da Hora Legal Brasileira, com rastreabilidade metrológica ao BIPM. Mantém e opera o Relógio Atômico, que é a Fonte Confiável do Tempo (FCT), a partir da qual se determina a Hora Legal Brasileira.
Octeto	Conjunto de 8 bits compreendendo um *byte*.
OCSP (On-line Certificate Status Protocol)	O Protocolo *On-line* para verificação de Estado de Certificados, OCSP é um dos dois esquemas comuns para verificar se um certificado digital não se encontra revogado. O outro método é a LCR (ver LCR).

PALAVRA CHAVE	DESCRIÇÃO
	Através do OCSP, qualquer aplicação pode fazer consultas a um serviço que checa, diretamente no Banco de Dados da Autoridade Certificadora, o status de um determinado certificado. As respostas emitidas por este serviço são individuais (uma para cada certificado) e são assinadas digitalmente, a fim de garantir sua confiabilidade. Dessa maneira, a lacuna entre o momento da revogação e a emissão da próxima LCR deixa de existir, já que, uma vez que seja marcado como revogado no banco de dados da AC, a próxima resposta OCSP já apresentará este status, eliminando a possibilidade de um acesso não-autorizado desta natureza.
Off-Line	Fora de linha, desligado. Quando não existe nenhum contato do computador com uma rede.
Oficial de Segurança	Papel de acesso que quando assumido por uma entidade usuária externa permite realizar serviços relacionados à iniciação do sistema de arquivos do módulo, gerenciamento do módulo, reinicialização do módulo, sobrescrita do valor de chaves criptográficas (*key zeroization*) e destruição do módulo.
On-Line	Significa "estar em linha", estar ligado em determinado momento à rede ou a um outro computador.
Operação Criptográfica	Operação que manipula uma chave criptográfica.
Operador	Um indivíduo ou processo que realiza operações no módulo criptográfico.
OpenSSL	É uma implementação de código aberto dos protocolos SSL e TLS. A biblioteca (escrita na linguagem C) implementa as funções básicas de criptografia e disponibiliza várias funções utilitárias. O *OpenSSL* está disponível para a maioria dos sistemas do tipo Unix, incluindo Linux, Mac OS X e para as quatro versões do BSD de código aberto e também para o *Microsoft Windows.*
Par de chaves	Chaves privada e pública de um sistema criptográfico assimétrico. A chave privada e sua chave pública são matematicamente relacionadas e possuem certas propriedades, entre elas a de que é impossível a dedução da chave privada a partir da chave pública conhecida. A chave pública pode ser usada para verificação de uma assinatura digital que a chave privada correspondente tenha criado ou a chave privada pode decifrar a uma mensagem cifrada a partir da sua correspondente chave pública. A chave privada deve ser de conhecimento exclusivo do titular do certificado.
Parâmetros críticos de segurança (PCS)	Representam informações sensíveis e relacionadas à segurança, tais como, chaves criptográficas assimétricas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja leitura ou modificação podem comprometer a segurança de um módulo criptográfico.
PEM (Privacy Enhanced Mail)	É um padrão da internet que fornece troca segura no correio eletrônico. O PEM emprega um conjunto de técnicas de criptografia para permitir a confidencialidade, a autenticação do remetente e a integridade da mensagem.

PALAVRA CHAVE	DESCRIÇÃO
	Os aspectos da integridade da mensagem permitem que o usuário assegure de que uma mensagem não seja modificada durante o transporte do remetente. A autenticação do remetente permite que um usuário verifique que a mensagem PEM que receberam é verdadeiramente da pessoa que reivindica tê-la emitido. A característica da confidencialidade permite que uma mensagem seja mantida secreta das pessoas a quem a mensagem não foi dirigida.
PI (Parte Interessada)	É a parte interessada (empresa) que deseja fazer a homologação junto ao LSITEC-LEA.
PIN (Personal Identification Number)	É uma seqüência de números e/ou letras (senha) usadas para liberar o acesso à chave privada, ou outros dados armazenados na mídia, somente para pessoas autorizadas.
PKCS (Public Key Cryptographic Standard)	Padrões de criptografia de chave pública. São especificações produzidas pelos Laboratórios RSA em cooperação com desenvolvedores de sistemas seguros de todo o mundo com a finalidade de acelerar a distribuição da criptografia de chave pública.
PKCS#1	Especificação de padrão de dados para o protocolo RSA, incluindo o padrão para criptografia e assinatura digital RSA e o padrão para estocagem de chaves públicas e privadas.
PKCS#5	Especificação de um padrão para derivação de chaves e mecanismos de cifração baseado em senhas. Descreve um método para cifrar um vetor de bytes utilizando uma chave secreta calculada a partir de uma senha (*Password-Based Encryption* ou PBE). É destinado á proteção de chaves privadas em situações que exijam a sua transferência. Isto pode ser necessário, por exemplo, quando as chaves são geradas pela CA e não pelo usuário; ou quando o usuário necessita transferir a chave para outra máquina. A cifragem utilizada está baseada no DES.
PKCS#10	Especificação de um padrão para codificar requisições de certificados, incluindo o nome da pessoa que requisita o certificado e sua chave pública.
PKCS#7 (CMS)	O padrão CMS descreve uma sintaxe genérica para dados que podem ser submetidos a funções criptográficas, tais como assinatura e envelopagem digital. Permite recursividade, com aninhamento de envelopes e *wrappers*. Permite também a associação de atributos arbitrários, como por exemplo selo temporal ou contra-assinatura, à mensagem no processo de autenticação por assinatura. Casos particulares oferecem meios de disseminação de certificados e CRLs. O padrão CMS pode dar suporte a uma variedade de arquiteturas de gerenciamento de chaves baseadas em ICP, como aquela proposta para o padrão PEM na RFC 1422. Entretanto, topologias, modelos de confiança e políticas de certificação para ICPs estão fora do seu escopo. Valores produzidos pelo padrão estão destinados à codificação DER, ou seja, para transmissão e armazenagem na forma de cadeias de octetos de comprimento não necessariamente conhecidos de antemão. Na ICP-Brasil, é largamente utilizado na assinatura digital.

PALAVRA CHAVE	DESCRIÇÃO
PKCS#8	Especificação de um padrão para chaves privadas: o valor da chave, o algoritmo correspondente e um conjunto de atributos associados. Define também em uma sintaxe para chaves cifradas recorrendo às técnicas PBE definidas no PKCS#5.
PKCS#11	Este padrão descreve a interface de programação chamada *"Cryptoki"* utilizada para operações criptográficas em hardwares: *tokens, smart cards*. É comum utilizar o PKCS#11 para prover o suporte aos *tokens* como as aplicações de SSL e S/MIME.
PKCS#12	Descreve uma sintaxe para a transferência de informação de identificação pessoal, incluindo chaves privadas, certificados, chaves secretas e extensões. É uma norma muito útil uma vez que é utilizada por diversas aplicações (ex. IE e Mozilla) para importar e exportar este tipo de informação. Suporta a transferência de informação pessoal em diferentes condições de manutenção da privacidade e integridade. O grau de segurança mais elevado prevê a utilização de assinaturas digitais e cifras assimétricas para proteção da informação.
PKI (Public Key Infrastrusture)	Infra-estrutura de chaves públicas. A ICP-Brasil é um exemplo de PKI.
Plano de Auditoria	Roteiro que descreve, pelo menos, como a auditoria pretende proceder à verificação da Política de Certificação, PC, da Declaração de Práticas de Certificação, DPC e da Política de Segurança, PS e recomendar providências quanto às observações levantadas.
Plano de Contingência	É um plano para situações de emergência, que visa a garantir a disponibilidade dos recursos e serviços críticos e facilitar a continuidade de operações de uma organização. Deve ser regularmente atualizado e testado, para ter eficácia caso necessária sua utilização. Sinônimo de plano de desastre e plano de emergência.
Plano de Continuidade de Negócios	Plano cujo objetivo é manter em funcionamento os serviços e processos críticos das entidades integrantes da ICP-Brasil, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.
Plano de Desenvolvimento e Implantação dos Trabalhos de Auditoria	Plano elaborado pela Empresa de Auditoria Independente, que especifica de maneira clara e objetiva cada etapa do trabalho, procedimentos e técnicas a serem adotadas em cada atividade, prazo de execução e pontos de homologação, bem como tabelas indicativas do número de horas de auditoria e o número de auditores a serem alocados nos serviços que serão realizados em entidades da ICP-Brasil.
Plano de Recuperação de Desastres	Conjunto de procedimentos alternativos, a serem adotados após um desastre, visando a reativação dos processos operacionais que tenham sido paralisados, total ou parcialmente, ainda que com alguma degradação.
Política de Carimbo de Tempo (PCT)	Conjunto de normas que indicam a aplicabilidade de um carimbo de tempo para uma determinada comunidade e/ou classe de aplicação com requisitos comuns de segurança.

PALAVRA CHAVE	DESCRIÇÃO
Política de Certificação (PC)	Documento que descreve os requisitos, procedimentos e nível de segurança adotados para a emissão, revogação e gerenciamento do ciclo de vida de um Certificado Digital.
Política de Segurança (PS)	É um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades.
Precisão	Ver Exatidão.
Prestador de Serviço de Certificação	As Autoridades Certificadoras, as Autoridades de Registro e os prestadores de serviço suporte credenciados junto à ICP-Brasil.
Prestador de Serviços de Suporte	Aquele que desempenha as atividades descritas na PC, PCT, DPC ou DPCT da AC ou ACT responsável por esses documentos. São empresas contratadas por uma AC, ACT ou AR para realizar atividades de: disponibilização de infra-estrutura física e lógica; disponibilização de recursos humanos especializados; disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.
Privacidade de documentos eletrônicos	Vide Confidencialidade de Documentos Eletrônicos
PRNG (Pseudo Random Number Generator)	Um gerador de número pseudo-aleatório é um algoritmo que gera uma seqüência de números, os quais são aproximadamente independentes um dos outros. A saída da maioria dos geradores de números aleatórios não é verdadeiramente aleatória; ela somente aproxima algumas das propriedades dos números aleatórios. Enquanto números verdadeiramente aleatórios podem ser gerados usando hardware para geração de número aleatório, número pseudo aleatórios são uma parte crítica da computação moderna, da criptografia até o método de *Monte Carlo* passando por sistemas de simulação. Uma cuidadosa análise matemática é necessária para assegurar que a geração dos números seja suficientemente "aleatória".
Procedimento de Fiscalização	As ações que objetivam a verificação do cumprimento das normas que regem a ICP-Brasil por parte das entidades credenciadas.
Protocolo	Uma descrição das regras que dois computadores devem obedecer ao estabelecer uma comunicação. Um conjunto de regras padronizadas que especifica o formato, a sincronização, o seqüenciamento, a transmissão de dados, incluindo inicialização, verificação, coleta de dados, endereçamento e verificação e correção de erros em comunicação de dados.
PSC (Provedor de Serviços Criptográficos)	Vide *CSP (Cryptographic Service Provider)*
Proxy	É um servidor que age como um intermediário entre uma estação de trabalho e a internet para segurança, controle administrativo e serviço de *cache*. Um servidor (programa) *proxy* (ou com capacidades de *proxy*) recebe pedidos de computadores ligados à sua rede e, caso necessário, efetua esses mesmos pedidos ao exterior dessa rede, usando como identificação o seu próprio numero IP e não o numero IP do computador que requisitou o serviço. Útil

PALAVRA CHAVE	DESCRIÇÃO
	quando não se dispõe de números IP registrados numa rede interna ou por questões de segurança.
PUK (Personal Identification Number Umblocking Key)	É uma chave para desbloqueio do número de identificação pessoal (PIN), o qual normalmente fica bloqueado após várias tentativas inválidas. Como o PIN, a senha PUK deve ser guardada de forma segura, pois ambas permitem, em dispositivos como *tokens* e *smart cards*, o acesso à chave privada de um titular de certificado.
Rastreabilidade	Relacionamento do resultado de uma medição de sincronismo com um valor de referência previamente estabelecido como padrão. A rastreabilidade se evidencia por intermédio de uma seqüência contínua de medidas, devidamente registradas e armazenadas e permite a verificação, direta ou indireta, do relacionamento entre o tempo informado e a fonte confiável de tempo.
Recuperação de Chave	Processo no qual uma chave privada pode ser recuperada, a partir de dados armazenados por uma empresa ou órgão governamental. Na ICP-Brasil é proibida a recuperação de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.
Rede	Um grupo de computadores inter-conectados, controlados individualmente, junto com o hardware e o software usado para conectá-los. Uma rede permite que usuários compartilhem dados e dispositivos periféricos como impressoras e mídia de armazenamento, troquem informações por meio do correio eletrônico e assim por diante.
Rede de Sincronismo Autenticado (ReTemp/HLB)	Rede criada e mantida pelo Observatório Nacional, que permite a rastreabilidade e a autenticação do tempo, nos equipamentos que a compõem, em relação à Hora Legal Brasileira e à UTC.
Rede Local	Um grupo de computadores conectados com a finalidade de compartilhar recursos. Os computadores em uma rede local são normalmente ligados por um único cabo de transmissão e localizados dentro de uma pequena área, como um único prédio ou seção de um prédio.
Redundância	i. Componentes de um sistema de computador que são instalados para fazer *backup*. Utilizados para garantir a operação ininterrupta de um sistema em caso de falha. ii. Diz-se de um segundo dispositivo que esteja imediatamente disponível para uso quando de uma falha de um dispositivo primário de um sistema de computador.
Registro	Cadeia de octetos que pode ser manuseada como um todo pelo cartão inteligente e referenciada por um número de registro ou por um identificador de registro [ISO/IEC 7816-4].
Relatório de auditoria	Documento que traduz a forma como foi desenvolvido o trabalho de auditoria e que exprime de forma clara, concisa e exata, uma opinião sobre os resultados a que o auditor chegou, devendo conter, sempre que for caso, as alegações, as respostas ou as observações dos responsáveis e, ainda, conclusões e recomendações.

PALAVRA CHAVE	DESCRIÇÃO
Relatório de Fiscalização	Documento pelo qual o servidor responsável pela fiscalização descreve o que constatou na entidade fiscalizada
Relying Party	Vide Terceira Parte
RNG (Random Number Generator)	Quando um número aleatório é gerado por um programa, este número não é exatamente aleatório (por isto que números aleatórios gerados por programas são mais corretamente classificados como pseudo-aleatórios). Portanto, em sistemas onde são geradas chaves criptográficas importantes, é necessário existir um circuito chamado *Random Number Generator* (RNG) que garanta que os números gerados são realmente ao acaso e não baseados no relógio de tempo real do computador.
Realimentação de dados de autenticação *(Echo)*	Exibição visível de caracteres no momento da inserção de uma senha.
Renovação de Certificados	É o processo para obter um certificado novo antes que o certificado existente tenha expirado. Na ICP-Brasil, é obrigatória a geração de novas chaves criptográficas para cada certificado emitido.
Repositório	É um sistema confiável e acessível *on-line,* mantido por uma Autoridade Certificadora, para publicar sua Declaração de Práticas de Certificação (DPC), Políticas de Certificado (PC), Política de Segurança (PS), Lista de Certificados Revogados (LCR) e endereços das instalações técnicas das AR vinculadas.
Resolução (*Resolution*)	Menor diferença entre indicações de um dispositivo mostrador que pode ser significativamente percebida. A resolução de um relógio é o menor incremento de tempo que o mesmo pode indicar.
Retardo (*Delay*)	Tempo de propagação na internet entre o SCT e o SAS.
Revogação de Certificados	Encerramento da validade de um certificado digital antes do prazo previsto. Pode ocorrer por iniciativa do usuário, da Autoridade de Registro, da Autoridade Certificadora ou da Autoridade Certificadora Raiz.
RFC (Request for Comments)	Os RFC são documentos técnicos ou informativos que discutem os mais diversos aspectos relacionados à internet. Os assuntos variam desde especificações, padrões e normas técnicas até questões históricas acerca da rede mundial de computadores. Os RFC são documentos públicos, qualquer pessoa tem acesso a eles, podendo ler, comentar, enviar sugestões e relatar experiências sobre o assunto. Pode-se pesquisar os RFC no *site*: http://www.faqs.org/rfcs.
Risco ou Ameaça	i. É a probabilidade da concretização de um evento que possa causar perdas significativas por causar danos a um ou mais aos ativos da organização. ii. É um fator externo que pode vir a atacar um ativo causando um desastre ou perda significativa.
Roteador	Sistema computacional que usa uma ou mais métricas para determinar o caminho otimizado pelo qual o tráfego da rede deve ser encaminhado – por meio de seus endereços – de uma rede local ou remota para outra.
Roteamento	Processo de seleção de rotas para uma mensagem.

PALAVRA CHAVE	DESCRIÇÃO
RSA (Rivest Shamir and Adleman)	O RSA é um algoritmo assimétrico que possui esse nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. É, atualmente, o algoritmo de chave pública mais amplamente utilizado, sendo capaz de fornecer assinaturas digitais e cifrar textos.
Sala-cofre	Área de Segurança restrita, formada por cofre com proteção eletromagnética, física e contra fogo, afim de proteger as chaves privativas que assinam os Certificados Digitais.
Secure Messaging **(Transferência Segura de Mensagens por Meios Eletrônicos)**	Qualquer método de entrega de uma mensagem segura, incluindo *TLS* (segurança da camada de transporte), SMTP sobre SSL e HTTPS.
Segundo de Transição ***(leap second)***	Ajuste ao UTC por meio da subtração ou adição de um segundo no último segundo de um mês do UTC. A primeira escolha é o fim de dezembro e de junho e a segunda escolha é o fim de março e de setembro.
Segurança Física	O principal objetivo da implantação de controles de segurança física é restringir o acesso às áreas críticas da organização, prevenindo os acessos não autorizados que podem acarretar danos a equipamentos, acessos indevidos à informação, roubos de equipamentos, entre outros. Os controles de acesso físico devem ser implementados em conjunto com os controles de acesso lógico. A falta de implementação desses dois controles em conjunto, seria o mesmo que restringir o acesso às informações através de senhas, mas deixar os servidores desprotegidos fisicamente, vulneráveis a roubo, por exemplo.
Selo Cronológico Digital	Serviço que registra, no mínimo, a data e a hora correta de um ato, além da identidade da pessoa ou equipamento que enviou ou recebeu o selo cronológico. O Selo Cronológico Digital cria uma confirmação assinada digitalmente e à prova de fraude sobre a existência de uma transação ou documento específico.
Selo de Homologação	Selo conferido aos sistemas e equipamentos homologados pelo ITI.
Semente (de chave criptográfica)	Um valor secreto usado para inicializar uma função ou uma operação criptográfica.
Senha	Um conjunto de caracteres, conhecidos apenas pelo usuário, que fornecem acesso ao arquivo, computador ou programa. Senhas são geralmente usadas em conjunto com o nome do usuário que o autentica e o garante autorização ao acesso.
Senha Forte	Inverso de Senha Fraca ou Óbvia
Senha Fraca ou Óbvia	É aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tal como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras com significado, dentre outras

PALAVRA CHAVE	DESCRIÇÃO
Serviço Criptográfico ICP (ou Aplicação ICP)	Aplicação de infra-estrutura de chaves públicas contextualizada para o âmbito da ICP-Brasil.
Servidor de Aplicativos	Sistema que realiza a interface entre o subscritor e o SCT. Encaminha as solicitações de carimbo de tempo ao SCT e em seguida devolve ao subscritor os carimbos de tempo ou mensagens de erro recebidos em resposta.
Servidor de Autenticação e Sincronismo (SAS)	Dispositivo constituído por *hardware* e *software* que audita e sincroniza SAS ou SCT. Deve possuir um HSM com relógio para sincronização e capacidade de processamento criptográfico para geração de chaves criptográficas e realização de assinaturas digitais.
Servidor de Carimbo de Tempo (SCT)	Dispositivo único constituído por *hardware* e *software* que gera os carimbos de tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.
SHA-1 (*Secure Hash Algorithm)*	O *Secure Hash Algorithm,* uma função de espalhamento unidirecional inventada pela NSA, gera um valor *hash* de 160 bits, a partir de um tamanho arbitrário de mensagem.
SHA-224, SHA-256,SHA-384 e SHA-512 (SHA-2 Family - Secure Hash Algorithm)	O NIST publicou quatro funções adicionais da família *SHA*, cada uma com valores *hash* maiores, conhecidos coletivamente como *SHA-2*. As variantes individuais são nomeadas, através de seus comprimentos de *hash* (em *bits*): SHA-224, SHA-256, SHA-384, e SHA-512. O SHA-224 foi definido para combinar o comprimento da chave com duas chaves TripleDES. SHA-256 e SHA-512 são funções de *hash* computadas com palavras de 32 bits e 64 bits respectivamente. Usam quantidades diferentes de deslocamento e constantes adicionais, mas suas estruturas são virtualmente idênticas, diferindo somente no número de voltas. SHA-224 e SHA-384 são simplesmente versões truncadas das duas primeiras, computadas com valores iniciais diferentes.
Sigilo	Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas. Os titulares de certificados de assinatura digital emitidos pela AC são responsáveis pela geração, manutenção e pela garantia do sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevidas dessas mesmas chaves.
Signatário	É a pessoa/entidade que cria uma assinatura digital para uma mensagem com a intenção de autenticá-la.
Signed Data	O tipo de conteúdo *signed data* consiste em um conteúdo de todos os tipos e zero ou mais valores de assinatura digital. Qualquer número de assinantes pode assinar em paralelo qualquer tipo de conteúdo. A aplicação típica do tipo de conteúdo *signed data* é representada por uma assinatura digital do assinador no conteúdo do tipo de conteúdo de dados. Uma outra aplicação típica disseminada são os certificados digitais e as listas da revogação do certificado (CRL).
Sincronização de	Processo pelo qual dois ou mais relógios passam a indicar o mesmo tempo.

PALAVRA CHAVE	DESCRIÇÃO
Relógio	
Sistema de Autenticação e Sincronismo (SAS)	Dispositivo constituído por hardware e software que audita e sincroniza SAS ou SCT. Deve possuir um HSM com relógio para sincronização e capacidade de processamento criptográfico para geração de chaves criptográficas e realização de assinaturas digitais.
Servidor de Carimbo de Tempo (SCT)	Dispositivo único constituído por hardware e software que emite os carimbos de tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.
Sistema Criptográfico	Sistema composto de documentação normativa específica de criptografia aplicada na ICP-Brasil, conjunto de requisitos de criptografia, projetos, métodos de implementação, módulos implementados de *hardware* e *software*, definições relativas a algoritmos criptográficos e demais algoritmos integrantes de um processo criptográfico, procedimentos adotados para gerência das chaves criptográficas, métodos adotados para testes de robustez das cifras e detecção de violações dessas.
Sistema de Certificação Digital	Todo e qualquer programa de computador, ainda que embarcado, que compõe meio necessário ou suficiente à realização de Certificação Digital.
Sistema de Detecção de Intruso (IDS)	Ferramentas de segurança que ajudam os administradores a evitarem danos na rede quando as outras proteções, tais como controle de acesso ou *firewalls*, não conseguem afastar os intrusos. Detecta tentativas ou ataques bem-sucedidos nos recursos monitorados. Os recursos monitorados podem fazer parte de uma rede ou um sistema *host*.
Sistema de Pagamento Brasileiro (SPB)	Sistema responsável pela interação entre o Banco Central, o governo, as instituições financeiras, as empresas e até mesmo as pessoas físicas. Gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, ligando as Instituições Financeiras credenciadas ao Banco Central do Brasil. Utiliza certificados digitais da ICP-Brasil para autenticar e verificar a identidade dos participantes em todas as operações realizadas;
Sistema Operacional	Programa principal que se dedica às tarefas de organização e controle das atividades do computador e seus periféricos.
Skew	Diferença de freqüência entre dois relógios (primeira derivada do *offset* no tempo).
Slot	Em um *HSM (Hardware Security Module)*, um *slot* é um leitor lógico que pontencialmente contém um *token.*
Smart Card	i. É um tipo de cartão plástico semelhante a um cartão de crédito com um ou mais *microchips* embutidos, capaz de armazenar e processar dados. Um *smart card* pode ser programado para desempenhar inúmeras funções, inclusive pode ter capacidade de gerar chaves públicas e privadas e de armazenar certificados digitais. Pode ser utilizado tanto para controle de acesso lógico como para controle de acesso físico.

PALAVRA CHAVE	DESCRIÇÃO
	ii. Um pequeno dispositivo, geralmente do tamanho de um cartão de crédito, que contém um processador e é capaz de armazenar informação criptográfica (como chaves e certificado) e realizar operações criptográficas.
S/MIME (Secure / Multipurpose Internet Mail Extensions)	*S/MIME* é um protocolo de segurança de *e-mail*. Foi desenhado para prevenir a interceptação e falsificação de *e-mail* usando cifração e assinatura digital. S/MIME constrói a segurança em cima do protocolo MIME e é baseado na tecnologia desenvolvida originalmente pela *RSA Data Security, Inc.*
SO	i. Sistema Operacional; ii. Em um *HSM (Hardware Security Module)*, é o *Security Officer,* é um usuário do dispositivo criptográfico com poderes de administrador do sistema.
Software	i. Programa de computador que utiliza uma seqüência lógica de instruções que o computador é capaz de executar para obter um resultado específico. ii. Conjunto de programas e instruções que operam o computador. São dois os tipos de *software* de computador: *software* de sistema, o qual engloba operações básicas necessárias para operar o *hardware* (por exemplo, sistema operacional, utilitários de comunicação, monitores de performance, editores, compiladores etc.) e *software* aplicativo, o qual executa tarefas específicas para auxiliar os usuários em suas atividades. iii. Programas e componentes de dados que podem ser dinamicamente modificados durante a execução, usualmente armazenados em mídias regraváveis.
SSL (Secure Socket Layer)	Protocolo de segurança que provê privacidade na comunicação através da internet. O Protocolo permite que aplicativos cliente e servidor se comuniquem utilizando mecanismos criados para proteger o sigilo e a integridade do conteúdo que trafega pela internet. Desenvolvido pela Netscape para transmitir documentos privativos pela internet.
Subscritor	Pessoa física ou jurídica que solicita os serviços de uma Autoridade de Carimbo do Tempo (ACT), implícita ou explicitamente concordando com os termos mediante os quais o serviço é oferecido.
Suspensão de Certificado	Suspensão do uso de um certificado digital por um período determinado de tempo. A suspensão de certificado digital não é permitida no âmbito da ICP-Brasil.
Switch	Dispositivo que direciona pacotes em uma rede.
Template	Na especificação do *PKCS#11 (Cryptoki),* um *template* é um vetor de atributos e é usado para criar, manipular e procurar objetos.
TRC (Teorema de Resto Chinês)	Este algoritmo, utilizado para resolver sistemas de congruências lineares, é muito antigo e foi inventado, independentemente, pelos chineses e pelos gregos, para resolver problemas de astronomia. O algoritmo chinês do resto tem este nome porque um dos primeiros lugares em que aparece é o livro *Manual de aritmética do mestre Sun*,

PALAVRA CHAVE	DESCRIÇÃO
	escrito entre 287 d.C. e 473 d.C.
Tempo Universal Coordenado (UTC)	Escala de tempo adotada como padrão de Tempo Oficial Internacional, utilizada pelo sistema de Metrologia Internacional, Convenção do Metro, determinada e disseminada pelo *Bureau International des Poids et Mesures* - BIPM, França.
Terceira Parte	i. É a parte que age confiante no teor, validade e aplicabilidade do certificado digital emitido por uma das AC integrantes da ICP-Brasil. ii. Pessoa ou instituição que age com total independência de fabricantes, desenvolvedores, representantes comerciais, prestadores de serviços de certificação digital e de potenciais compradores de sistemas e equipamentos de certificação digital
Termo de Responsabilidade	Termo assinado por uma pessoa física, que será a responsável pelo uso do certificado, quando o titular do certificado é uma organização. No termo, estão estabelecidas as condições de uso do certificado.
Termo de Titularidade	Termo assinado pelo titular do certificado digital emitido para pessoa física ou jurídica onde são estabelecidas as condições de uso do mesmo.
Termo Inicial de Fiscalização (TIF)	O documento que inicia o procedimento de fiscalização.
Texto Cifrado	Dado que foi criptografado. O texto cifrado é a saída do processo de criptografia e pode ser transformado novamente em informação legível em forma de texto claro a partir da chave de decifração.
Texto Claro	Dado que está no estado não cifrado ou decifrado.
Thread-safe	É um conceito de programação de computador aplicado ao contexto de programas *multi-threaded*. Uma parte do código é t*hread-safe* se funcionar corretamente durante a execução simultânea para *threads* múltiplas. Em particular, deve satisfazer à necessidade para *threads* múltiplas para acessar os mesmos dados compartilhados e a necessidade para uma parte compartilhada dos dados ser acessada por somente uma *thread* de cada vez.
Time-stamping	Vide Datação de Registros
Tipo de Certificados	Na ICP-Brasil estão definidos oito (08) tipos de certificados para titulares, classificados da seguinte forma: A1, A2, A3, A4, S1, S2, S3 e S4 e um tipo de certificado para Autoridades Certificadoras.
Titular de Certificado	São as entidades, pessoa física ou jurídica, para as quais foram emitidos um certificado digital. O assinante é o titular da chave privada correspondente à chave pública contida no certificado e possui a capacidade de utilizar tanto uma quanto a outra.
Token	i. Dispositivo para armazenamento do Certificado Digital de forma segura, sendo seu funcionamento parecido com o *smart card,* tendo sua conexão com o computador via USB. ii. Em um *HSM (Hardware Security Module),* um *token* é a visão lógica de

PALAVRA CHAVE	DESCRIÇÃO
	um dispositivo criptográfico definido em *PKCS#11 (Cryptoki).*
Topologia	Disposição física dos nós e dos meios de rede dentro de uma estrutura de rede corporativa.
Transporte de Chaves (*Key Transport*)	Processo ou protocolo que possibilita que uma chave criptográfica simétrica compartilhada seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.
Trilhas de Auditoria	i. Histórico das transações de sistemas que estão disponíveis para a avaliação com o objetivo de provar a correção de sua execução comparada com os procedimentos ditados pela política de segurança. ii. rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. iii. conjunto cronológico de registros que proporcionam evidências do funcionamento do sistema. Estes registros podem ser utilizados para reconstruir, revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para rastrear o uso do sistema, detectando e identificando usuários não autorizados.
Triple DES (3DES)	O 3DES é uma variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar um versão com duas ou com três chaves diferentes. Seu tamanho de chave é de 112 ou 168 bits.
Unidade de Dado	No contexto da norma ISO 7816-4 representa o menor conjunto de bits que pode ser referenciado de forma não ambígua [ISO/IEC 7816-4].
URL (Uniform Resource Locator)	Um mecanismo padronizado para identificar e localizar certos cadastros e outros recursos localizados na *World Wide Web*. A maioria das URLs aparece na forma familiar de endereços de sites.
Usuário	i. Pessoa que utiliza certificado digital apresentado por um titular. ii. Papel de acesso que quando assumido por uma entidade usuária externa permite realizar serviços de segurança no módulo criptográfico após sua iniciação, incluindo operações criptográficas, geração de chaves criptográficas, o uso do sistema de arquivos, sobrescrita do valor de chaves criptográficas (*key zeroization*), etc.
Usuário Final	É uma pessoa física ou jurídica que possui um certificado digital. Sinônimo de Titular de Certificado.
Validação da Cadeia de Certificados	Consiste na verificação da validade do certificado, nomeadamente a data, assinatura e validade dos certificados que estejam na sua cadeia de certificação, até ao certificado de confiança.
Validade de LCR	Período de tempo em que a LCR está com sua data de validade operacional. As LCR possuem prazo máximo de validade de acordo com o tipo de certificado previsto na ICP-Brasil.
Validade do Certificado	Período de tempo em que o certificado está com sua data de validade operacional. Os Certificados possuem prazo máximo de validade de acordo

PALAVRA CHAVE	DESCRIÇÃO
	com o tipo de certificado previsto na ICP-Brasil.
Verificação	Ratificação da identidade de uma pessoa física ou jurídica mediante a solicitação de certificado através de documentação apresentada pelo solicitante e da reconfirmação dos dados da solicitação.
Verificação da Validade do Certificado	Processo realizado por um destinatário ou terceira parte para confirmar que o certificado de um titular, usuário final, é válido e era operacional na data e hora que uma assinatura digital pertinente foi criada.
Verificação de Assinatura digital	Ação realizada para determinar com precisão que: i. a assinatura digital foi criada durante o período operacional de um certificado válido por uma chave privada correspondente à chave pública contida no certificado e ii. que a mensagem associada não tenha sido alterada desde que a assinatura digital foi criada.
Vírus	Os vírus são pequenos segmentos de códigos programados, normalmente com más intenções, que têm a característica de se agregar ao código de outros programas. Assim que são executados, disparam o código maliciosamente alterado a fim de causar modificações indevidas no processamento normal do sistema em que este se encontra, causando (ou não) desde danos leves a irreparáveis.
VPN (Virtual Private Networks)	É definida como a conectividade de uma corporação e suas unidades através de uma infra-estrutura compartilhada de comunicação com as mesmas características de segurança de uma rede privativa. Os nós são conectados por meio de recursos de uma rede pública de telecomunicações, utilizando criptografia e outros dispositivos de segurança para garantir que os dados dessa rede não serão interceptados.
Vulnerabilidade	É uma fraqueza em uma máquina, programa ou sistema que pode ser explorada por um agressor. Agressores procuram por essas vulnerabilidades para explorá-las como forma de tomar acesso ao sistema. Um bom administrador de redes se mantém informado e atualizado de todas as vulnerabilidades descobertas nos sistemas, para agir de forma rápida na correção daquelas que dizem respeito ao ambiente que administra.
Worms	São programas maliciosos semelhantes aos vírus, porém se diferenciam na forma de infecção e nos tipos de danos que podem causar.
X.509	Recomendação ITU-T, a especificação X.509 é um padrão que especifica o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública, permitindo autenticação forte. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseadas em nomes distintos para localização. Na ICP-Brasil utilizam-se certificados no padrão X-509 V3.
Zeramento de Chaves	Vide *Key Zeroization*