## 1.1 Definições, acrônimos e abreviações

**AC:** Autoridade Certificadora

**Armazenamento:**Guarda de documentos em local apropriado Storage.

**Arquivo digital:** Conjunto de bits que formam uma unidade lógica interpretável por um programa de computador e armazenada em suporte apropriado.

**Assinatura digital:** O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de hash

- **autenticidade** - o receptor deve poder confirmar que a assinatura foi feita pelo emissor;
- **integridade** - qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;
- **não repúdio ou irretratabilidade** - o emissor não pode negar a autenticidade da mensagem.

**Autoridade Certificadora (AC):**Organização que emite certificados digitais obedecendo às práticas definidas na Infra-estrutura de Chaves-Públicas - ICP.

**ASES:** Tendo por objetivo fornecer instrumentos que viabilizem a adoção da acessibilidade pelos órgãos do governo, o ASES é uma ferramenta que permite avaliar, simular e corrigir a acessibilidade de páginas, sítios e portais, sendo de grande valia para os desenvolvedores e publicadores de conteúdo.

**Base de dados:** Conjunto de dados estruturados, com as respectivas regras de acesso, formatação e validação e gerenciados por um Sistema Gerenciador de Banco de Dados – SGBD.

**Carimbo de tempo:** Código binário, ligado a um documento, que registra a data e hora em que ocorreu um evento, como criação, recebimento, leitura, modificação ou eliminação. É uma forma de autenticação do documento ( Time-stamp)

**Certificação digital:** O certificado digital é um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos

**Chave privada:** Chave matemática formada por uma seqüência de dígitos, usada para criptografia assimétrica e criada em conjunto com a chave pública correspondente que deve ser mantida em segredo pelo

portador. Usada para assinar digitalmente documentos, bem como para decifrar aqueles criptografados com a chave pública correspondente.

**Chave pública:** Chave matemática formada por uma seqüência de dígitos, usada para criptografia assimétrica e criada em conjunto com a chave privada correspondente, disponibilizada publicamente por certificado digital, e utilizada para verificar assinaturas digitais. Também pode ser usada para criptografar mensagens ou arquivos a serem decifrados com a chave privada correspondente.

**Criptografia:** Método de codificação de dados segundo algoritmo específico e chave secreta de forma que somente os usuários autorizados podem restabelecer sua forma original.

**Criptografia assimétrica:** Método de criptografia que utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par. As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. (ITI)

**Eping:** Padrões de Interoperabilidade de Governo Eletrônico - é um projeto criado há cerca de um ano pelo Governo Federal junto a outros órgãos de governo

**Firewall ou Ipetables:** é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

**Hd** : Hard disk drive

**ISO27002:** A norma ISO 27001 é uma norma internacional que possibilita às organizações a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), através do estabelecimento de uma política de segurança, controles e gerenciamento de riscos.

**IPS:** Um sistema de prevenção de intruso ( **Intrusion Prevention System**) é um dispositivo de segurança de rede que monitora o tráfego e/ou atividades dos sistema em busca de comportamentos maliciosos ou não desejáveis, em tempo real, para bloquear ou prevenir essas atividades.

**jQuery** : é um framework para ajudar os desenvolvedores

**Linux:** Linux é o termo geralmente usado para designar qualquer sistema operativo ou sistema operacional que utilize o núcleo Linux.
**Mysql**: O MySQL é um sistema de gerenciamento de banco de dados (SGBD), que utiliza a linguagem SQL (Linguagem de Consulta Estruturada, do inglês Structured Query Language) como interface

**NIDS**: (Network Intrusion Detection System) snort é um software livre de detecção de intrusão para rede (NIDS)

**Nessus:** é um programa de verificação de falhas/vulnerabilidades de segurança.

**NFS: nfs** (acrônimo para Network File System) é um sistema de arquivos distribuídos desenvolvido inicialmente pela Sun Microsystems, Inc., a fim de compartilhar arquivos e diretórios entre computadores conectados em rede, formando assim um diretório virtual.

**Raid**: Redundant Array of Inexpensive Drives (discos independentes)

**Sistema Operacional VM Foundation:** A empresa de virtualização VMware é a última empresa a juntar-se à Linux Foundation, uma organização internacional dedicada a acelerar o crescimento do Linux. Enquanto há várias empresas juntas com a Linux Foundation, a empresa VMware para o *cloud computing*.

**VPN :** Virtual Private Network (VPN), ou Rede Privada Virtual, é um túnel virtual privativo construído sobre a infra-estrutura de uma rede pública ou privada. Em vez de se utilizar circuitos dedicados ou redes de pacotes para conectar redes remotas, utiliza-se usualmente a infra-estrutura da Internet.

**Web fone:** VOIP Telefone para fazer ligação pelo site ( onde o cliente cartório ou instituição para suporete).

**Zabbix:** Zabbix é uma solução open source de monitoramento para servidores, serviços e dispositivos de rede.

**Zend Framework :** O framework é um conjunto de classes com objetivo de reutilização de um design, provendo um guia para uma solução de arquitetura em um domínio específico de software.