Presidência da República
Casa Civil da Presidência da República

TERMO DE REFERÊNCIA

CG ICP-BRASIL

COMITÊ GESTOR DA ICP-BRASIL

1. Introdução

O Comitê Gestor da ICP-Brasil (CG ICP-Brasil) é a entidade máxima, integrante da arquitetura da Infra-estutura de Chave Pública Brasileira - ICP-Brasil, responsável pelo estabelecimento e administração das políticas a serem seguidas pelas Autoridades Certificadoras - AC integrantes desta estrutura. O CG ICP-Brasil é um órgão colegiado integrado por representantes do governo e do setor privado, conforme descrito na Medida Provisória 2200, de 28 de junho de 2001.

A ICP-Brasil é um conjunto de técnicas, práticas e procedimentos com o objetivo de fornecer suporte à implementação e à operação de um sistema de certificação digital baseado em criptografia de chave pública.

O Termo de Referência do CG ICP-Brasil surgiu da necessidade de definição de um arcabouço de normatização institucional que detalhasse as suas funções, atribuições, competências e organização funcional.

2. Princípios da ICP-Brasil

A ICP-Brasil deve satisfazer a um determinado conjunto de princípios básicos de forma a garantir a sua eficácia.

2.1 Princípio da Responsabilização

A responsabilidade e a responsabilização dos proprietários, prestadores de serviço e usuários de sistemas de informação e outras partes envolvidas com a segurança dos sistemas de informação devem ser explicitas e documentadas.

2.2 Princípio do Conhecimento

A fim de fomentar a confiança nos sistemas de informação que formarão a ICP-Brasil, os proprietários, prestadores de serviço e usuários dos sistemas de informação e outras partes envolvidas, devem prontamente, e de maneira consistente com a manutenção da segurança, adquirir conhecimentos apropriados da existência e da abrangência geral das medidas, práticas e procedimentos relacionados à segurança dos sistemas de informação, mantendo-se informados sobre esse conjunto normativo.

2.3 Princípio da Ética

Os sistemas de informação que integrarão a ICP-Brasil e os seus mecanismos de segurança deverão ser fornecidos e utilizados de maneira tal que os direitos e interesses legítimos de outrem sejam respeitados.

2.4 Princípio da Multidisciplinaridade

As normas, práticas e procedimentos relacionados com a segurança dos sistemas de informação integrantes da ICP-Brasil deverão considerar os pontos de vista relevantes, inclusive os técnicos, administrativos, organizacionais, operacionais, comerciais, educacionais e jurídicos, tratando cada um destes de forma adequada.

2.5 Princípio da Proporcionalidade

A ICP-Brasil deverá contemplar níveis de segurança, normas, práticas e procedimentos compatíveis com a criticidade, a importância e o valor dos sistemas de informação que a utilizem, considerando-se os ambientes específicos envolvidos.

2.6 Princípio da Integração

As normas, práticas e procedimentos relacionados à segurança dos sistemas de informação deverão ser coordenados e integrados de modo a se criar um conjunto harmônico e coerente de segurança da informação para o governo e sociedade civil.

2.7 Princípio da Atualização

A segurança dos sistemas de informação integrantes da ICP-Brasil deverá ser reavaliada periodicamente, na medida em que os sistemas de informação e as exigências ligadas à sua segurança variam em relação ao tempo e momento tecnológico considerado.

2.8 Princípio da Escalabilidade

A perspectiva de crescimento que abrange tanto o número de aplicações quanto à quantidade de usuários.

2.9 Princípio da Interoperabilidade

Os sistemas que compõem a ICP-Brasil preferencialmente devem obedecer ao paradigma de sistemas abertos de modo a se reduzir ao máximo as incertezas relacionadas com a integração de outros sistemas à infra-estrutura existente.

3. Requisitos para implementação da ICP-Brasil

A base material e técnica da ICP-Brasil será formada por um conjunto de hardware, software, políticas e procedimentos, que dará forma à sua arquitetura.

Essa base será formada de um conjunto de políticas de segurança, políticas de certificados, práticas e regras operacionais, autoridade(s) certificadora(s),

autoridade(s) registradora(s), um sistema de distribuição de certificados e ainda um conjunto de aplicações adequadas e em conformidade com o uso dos recursos da ICP-Brasil.

3.1 A política de segurança

Estabelece as regras e diretrizes de segurança que deverão ser adotadas pelas diversas entidades que farão parte da ICP-Brasil. É composta por fundamentos que darão origem a procedimentos de segurança que definirão a forma como as entidades tratarão a informação, considerando as particularidades de cada ambiente. Incluirá ainda padrões que definirão como as entidades tratarão as chaves e informações sob sua guarda. Este conjunto definirá os controles necessários à segurança da informação. A política de segurança trata ainda da contingência e da auditoria dos diversos processos e atos administrativos da ICP-Brasil.

O desenvolvimento da política de segurança da ICP-Brasil deve considerar:

I. A legislação vigente;
II. As normas, os métodos e os códigos de práticas de abrangência mundial;
III. A promoção do conhecimento e experiência especializada e de melhores práticas em assuntos relacionados com a segurança da informação;
IV. A formação e o controle de validade de contratos e outros documentos firmados, mantidos e implementados nos sistemas de informação;
V. A análise de riscos e a definição de responsabilidade por falhas na segurança dos sistemas de informação da ICP-Brasil;
VI. As sanções penais, administrativas e outras relacionadas ao uso indevido dos sistemas de informação da ICP-Brasil;
VII. Os meios de obtenção de provas e trilhas de auditoria em sistemas de informação integrantes da ICP-Brasil;
VIII. A capacitação de especialistas e auditores na segurança dos sistemas de informação integrantes da ICP-Brasil.

3.2 As declarações de regras operacionais (DRO)

São documentos com níveis de detalhamento específicos, que conterão os procedimentos operacionais relacionados às políticas de segurança adotadas e políticas de certificados, e ainda como estas serão suportadas nos diversos ambientes operacionais. Incluirão definições sobre como as autoridades certificadoras serão implantadas e operadas, como os certificados serão emitidos, aceitos e revogados, como as chaves serão geradas, registradas, certificadas e mantidas.

3.3 A autoridade certificadora raiz (AC Raiz)

A AC Raiz, executora das políticas estabelecidas pelo CG ICP-Brasil, compete realizar o licenciamento das AC, emitir, manter e cancelar os certificados das AC, gerenciar a LCR e excutar atividades de fiscalização e auditoria em conformidade com as diretrizes estabelecidas pelo CG ICP-Brasil.

3.4 A autoridade certificadora (AC)

Funcionará como base material e técnica da confiança da ICP-Brasil, já que esta irá gerenciar os certificados de chave pública em todo o seu ciclo de vida. Considerando que um certificado digital é capaz de relacionar a identidade de um usuário ou sistema a uma determinada chave pública correlacionada a uma assinatura digital, a autoridade certificadora será responsável pela emissão de certificado digital, pelo agendamento da data de expiração do certificado e pela publicação dos certificados revogados na Lista de Certificados Revogados (LCR).

3.5 A autoridade registradora (AR)

A AR implementará a interface entre o usuário e a autoridade certificadora. A sua principal função será a identificação dos usuários, validação da solicitação e a submissão da solicitação de certificado à autoridade certificadora.

3.6 O sistema de distribuição de certificados

O sistema de distribuição de certificados será dependente do tipo de certificado a ser emitido, estabelecido pela política de certificados da respectiva AC, podendo ser estabelecido um mecanismo on-line de distribuição (página Web, serviço de correio eletrônico ou serviço de diretório), ou mídia entregue pela AR.