



**Política de Certificado de Assinatura Digital
do tipo A3 da Autoridade Certificadora
VALID BRASIL**

Sumário – PC A3 da AC VALID BRASIL

1. INTRODUÇÃO	5
1.1. Visão Geral.....	5
1.2. Identificação	5
1.3. Comunidade e Aplicabilidade.....	5
1.3.1. Autoridades Certificadoras.....	5
1.3.2. Autoridades de Registro	5
1.3.3. Prestador de Serviços de Suporte	6
1.3.3A. Prestadores de Serviço de Confiança.....	6
1.3.4. Titulares de Certificado	6
1.3.5. Aplicabilidade	7
1.4. Dados de Contato	7
2. DISPOSIÇÕES GERAIS.....	7
2.1. Obrigações e direitos.....	8
2.2. Responsabilidades.....	8
2.3. Responsabilidade Financeira	8
2.4. Interpretação e Execução.....	8
2.5. Tarifas de Serviço	8
2.6. Publicação e Repositório	8
2.7. Auditoria e Fiscalização	8
2.8. Sigilo	8
2.9. Direitos de Propriedade Intelectual	8
3. IDENTIFICAÇÃO E AUTENTICAÇÃO	8
3.1. Registro Inicial	8
3.2. Geração de novo par de chaves antes da expiração do atual.....	9
3.3. Geração de novo par de chaves após expiração ou revogação	9
3.4. Solicitação de Revogação	9
4. REQUISITOS OPERACIONAIS.....	9
4.1. Solicitação de Certificado	9
4.2. Emissão de Certificado	9
4.3. Aceitação de Certificado.....	9
4.4. Suspensão e Revogação de Certificado.....	9
4.5. Procedimentos de Auditoria de Segurança.....	9
4.6. Arquivamento de Registros.....	10
4.7. Troca de chave	10

4.8. Comprometimento e Recuperação de Desastre	10
4.9. Extinção dos serviços de AC, AR ou PSS	10
5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL	10
5.1. Controles Físicos.....	10
5.2. Controles Procedimentais	10
5.3. Controles de Pessoal	10
6. CONTROLES TÉCNICOS DE SEGURANÇA.....	10
6.1. Geração e Instalação do Par de Chaves	11
6.1.1. Geração do par de chaves	11
6.1.2. Entrega da chave privada à entidade titular	12
6.1.3. Entrega da chave pública para o emissor de certificado.....	12
6.1.4. Disponibilização de chave pública da AC VALID BRASIL para usuários	12
6.1.5. Tamanhos de chave.....	12
6.1.6. Geração de parâmetros de chaves assimétricas.....	12
6.1.7. Verificação da qualidade dos parâmetros.....	12
6.1.8. Geração de chave por <i>hardware</i> ou <i>software</i>	13
6.1.9. Propósitos de uso de chave (conforme o campo “ <i>key usage</i> ” na X.509 v3).....	13
6.2. Proteção da Chave Privada.....	13
6.2.1. Padrões para módulo criptográfico.....	13
6.2.2. Controle “n de m” para chave privada.....	13
6.2.3. Custódia (<i>escrow</i>) de chave privada.....	13
6.2.4. Cópia de segurança (<i>backup</i>) de chave privada	13
6.2.5. Arquivamento de chave privada	13
6.2.6. Inserção de chave privada em módulo criptográfico.....	14
6.2.7. Método de ativação de chave privada	14
6.2.8. Método de desativação de chave privada	14
6.2.9. Método de destruição de chave privada.....	14
6.3. Outros Aspectos do Gerenciamento do Par de Chaves	14
6.3.1. Arquivamento de chave pública.....	14
6.3.2. Períodos de uso para as chaves pública e privada	14
6.4. Dados de Ativação.....	14
6.4.1. Geração e instalação dos dados de ativação.....	14
6.4.2. Proteção dos dados de ativação.....	14
6.4.3. Outros aspectos dos dados de ativação	15
6.5. Controles de Segurança Computacional	15
6.5.1. Requisitos técnicos específicos de segurança computacional	15
6.5.2. Classificação da segurança computacional	15

6.6. Controles Técnicos do Ciclo de Vida.....	15
6.6.1. Controles de desenvolvimento de sistema	15
6.6.2. Controles de gerenciamento de segurança	15
6.6.3. Classificações de segurança de ciclo de vida.....	16
6.7. Controles de Segurança de Rede.....	16
6.8. Controles de Engenharia do Módulo Criptográfico.....	16
7. PERFIS DE CERTIFICADO E LCR.....	16
7.1. Perfil do Certificado.....	16
7.1.1. Número de versão	16
7.1.2. Extensões de certificado.....	16
7.1.3. Identificadores de algoritmo	19
7.1.4. Formatos de nome	19
7.1.5. Restrições de nome	20
7.1.6. OID (<i>Object Identifier</i>) de Política de Certificado	21
7.1.7. Uso da extensão “Policy Constraints”	21
7.1.8. Sintaxe e semântica dos qualificadores de política.....	21
7.1.9. Semântica de processamento para extensões críticas	21
7.2. Perfil de LCR.....	21
7.2.1. Número de versão	21
7.2.2. Extensões de LCR e de suas entradas.....	21
8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO	22
8.1. Procedimentos de mudança de especificação	22
8.2. Políticas de publicação e notificação.....	22
8.3. Procedimentos de aprovação.....	22
9. DOCUMENTOS REFERENCIADOS	22
10. LISTA DE ACRÔNIMOS	22

Autor: Valid Certificadora Digital Ltda.

Edição: Março de 2019

Versão: 5.1

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos mínimos na elaboração das suas Políticas de Certificado (PC), observados obrigatoriamente pela Autoridade Certificadora VALID BRASIL, AC integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1.2. Toda PC elaborada no âmbito da ICP-Brasil adota obrigatoriamente a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1].

1.1.3. O certificado emitido sob esta PC é do tipo A3.

1.1.4. Não se aplica.

1.1.5. Não se aplica.

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.1.8. Não se aplica.

1.2. Identificação

1.2.1. Esta PC é denominada 'Política de Certificado de Assinatura Digital do tipo A3 da AC VALID BRASIL' e referida como 'PC A3 da AC VALID BRASIL', sob o OID (*Object Identifier*): 2.16.76.1.2.3.35.

1.2.2. Tabela do OID atribuído a esta PC após conclusão do processo de credenciamento da AC VALID BRASIL no âmbito da ICP-Brasil:

Tipo do Certificado	OID
A3	2.16.76.1.2.3.35

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC refere-se à AC VALID BRASIL, (Avenida Paulista, nº 2064, 15º andar, São Paulo, SP, CEP: 01310-928 sob CNPJ 14.121.957/0001/09), integrante da ICP-Brasil.

1.3.1.2. As práticas e procedimentos de certificação da AC VALID BRASIL estão descritos no documento 'Declaração de Práticas de Certificação' da AC VALID BRASIL (DPC da AC VALID BRASIL).

1.3.2. Autoridades de Registro

1.3.2.1. Em nosso endereço eletrônico <http://www.validcertificadora.com.br>, estão publicados os dados a seguir, referentes às Autoridades de Registro (ARs) utilizadas pela AC VALID BRASIL para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

- a) relação de todas as ARs credenciadas, com informações sobre as PCs que implementam;
- b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
- c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
- d) relação de AR que tenham se descredenciado da cadeia da AC VALID BRASIL, com respectiva data do descredenciamento;
- e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
- f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICP-Brasil, se for o caso.

1.3.2.2. A AC VALID BRASIL mantém as informações acima sempre atualizadas.

1.3.3. Prestador de Serviços de Suporte

1.3.3.1. No endereço eletrônico <https://www.validcertificadora.com.br/index.aspx?DID=301> constam os Prestadores de Serviço de Suporte – PSS, vinculados à AC VALID BRASIL.

1.3.3.2. PSS são entidades utilizados pela AC VALID BRASIL e/ou suas ARs vinculadas para desempenhar atividade descrita nesta PC e DPC implementada pela AC VALID BRASIL, e se classificam em três categorias conforme o tipo de atividade prestada:

- a) disponibilização de infraestrutura física e lógica;
- b) disponibilização de recursos humanos especializados; ou
- c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC VALID BRASIL mantém as informações acima sempre atualizadas.

1.3.3A. Prestadores de Serviço de Confiança

1.3.3A.1. A relação dos Prestadores de Serviço de Confiança – PSC vinculados diretamente a AC VALID BRASIL está publicada no endereço eletrônico <https://www.validcertificadora.com.br/index.aspx?DID=301>.

1.3.3A.2. PSC são entidades utilizadas pelas ACs, ou a própria AC VALID BRASIL, nesta PC ou na DPC implementada pela AC VALID BRASIL e se classificam em três categorias, conforme o tipo de atividade prestada:

- a) armazenamento de chaves privadas dos usuários finais; ou
- b) serviço de assinatura digital, verificação da assinatura digital; ou
- c) ambos.

1.3.4. Titulares de Certificado

Podem ser titulares de certificados do tipo A3 emitidos segundo esta PC pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras.

Nota 1: No caso de certificado emitido para pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Nota 2: No caso de certificado emitido para aplicação, o titular será a pessoa jurídica solicitante do certificado.

1.3.5. Aplicabilidade

1.3.5.1. Esta PC emite exclusivamente certificados para as aplicações de Assinatura Geral. Os certificados podem ser utilizados em aplicações para confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.2. As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido pela AC VALID BRASIL, devidamente credenciada pela AC Raiz.

1.3.5.3. A AC VALID BRASIL leva em conta o nível de segurança previsto para o tipo do certificado na definição das aplicações para o certificado, nesta PC. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado.

1.3.5.4. Certificados de tipo A3 emitidos pela AC VALID BRASIL serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.5. Não se aplica.

1.3.5.6. Não se aplica.

1.3.5.7. Não se aplica.

1.3.5.8. Não se aplica.

1.4. Dados de Contato

Esta PC é administrada por:

Empresa: Valid Certificadora Digital Ltda.

Endereço: Avenida Paulista, nº 2064, 15º Andar, São Paulo, SP - Brasil

CEP: 03310-928

Página da Web: <http://www.validcertificadora.com.br/>

Área: Normas e Compliance

Telefone: +55 11 2575-6800

Mail: pki.compliance@valid.com

2. DISPOSIÇÕES GERAIS

Os itens seguintes são referidos aos correspondentes da DPC da AC VALID BRASIL.

2.1. Obrigações e direitos

- 2.1.1. Obrigações da AC VALID BRASIL
- 2.1.2. Obrigações das ARs
- 2.1.3. Obrigações do Titular do Certificado
- 2.1.4. Direitos da terceira parte (*Relying Party*)
- 2.1.5. Obrigações do Repositório

2.2. Responsabilidades

- 2.2.1. Responsabilidades da AC VALID BRASIL
- 2.2.2. Responsabilidades da AR

2.3. Responsabilidade Financeira

- 2.3.1. Indenizações devidas pela terceira parte (*Relying Party*)
- 2.3.2. Relações Fiduciárias
- 2.3.3. Processos Administrativos

2.4. Interpretação e Execução

- 2.4.1. Legislação
- 2.4.2. Forma de interpretação e notificação
- 2.4.3. Procedimentos de solução de disputa

2.5. Tarifas de Serviço

- 2.5.1. Tarifas de emissão e renovação de certificados
- 2.5.2. Tarifas de acesso a certificados
- 2.5.3. Tarifas de revogação ou de acesso à informação de status
- 2.5.4. Tarifas para outros serviços
- 2.5.5. Política de reembolso

2.6. Publicação e Repositório

- 2.6.1. Publicação de informação da AC VALID BRASIL
- 2.6.2. Frequência de publicação
- 2.6.3. Controles de acesso
- 2.6.4. Repositórios

2.7. Auditoria e Fiscalização

2.8. Sigilo

- 2.8.1. Tipos de informações sigilosas
- 2.8.2. Tipos de informações não sigilosas
- 2.8.3. Divulgação de informação de revogação e de suspensão de certificado
- 2.8.4. Quebra de sigilo por motivos legais
- 2.8.5. Informações a terceiros
- 2.8.6. Divulgação por solicitação do titular
- 2.8.7. Outras circunstâncias de divulgação de informação

2.9. Direitos de Propriedade Intelectual

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes são referidos aos correspondentes da DPC da AC VALID BRASIL.

3.1. Registro Inicial

- 3.1.1. Disposições Gerais
- 3.1.2. Tipos de nomes

- 3.1.3. Necessidade de nomes significativos
- 3.1.4. Regras para interpretação de vários tipos de nomes
- 3.1.5. Unicidade de nomes
- 3.1.6. Procedimento para resolver disputa de nomes
- 3.1.7. Reconhecimento, autenticação e papel de marcas registradas
- 3.1.8. Método para comprovar a posse de chave privada
- 3.1.9. Autenticação da identidade de um indivíduo
- 3.1.10. Autenticação da identidade de uma organização
- 3.1.11. Autenticação da identidade de equipamento ou aplicação

3.2. Geração de novo par de chaves antes da expiração do atual

3.3. Geração de novo par de chaves após expiração ou revogação

3.4. Solicitação de Revogação

4. REQUISITOS OPERACIONAIS

Os itens seguintes são referidos aos correspondentes da DPC da AC VALID BRASIL.

4.1. Solicitação de Certificado

4.2. Emissão de Certificado

4.3. Aceitação de Certificado

4.4. Suspensão e Revogação de Certificado

- 4.4.1. Circunstâncias para revogação
- 4.4.2. Quem pode solicitar revogação
- 4.4.3. Procedimento para solicitação de revogação
- 4.4.4. Prazo para solicitação de revogação
- 4.4.5. Circunstâncias para suspensão
- 4.4.6. Quem pode solicitar suspensão
- 4.4.7. Procedimento para solicitação de suspensão
- 4.4.8. Limites no período de suspensão
- 4.4.9. Frequência de emissão de LCR
- 4.4.10. Requisitos para verificação de LCR
- 4.4.11. Disponibilidade para revogação ou verificação de status *on-line*
- 4.4.12. Requisitos para verificação de revogação *on-line*
- 4.4.13. Outras formas disponíveis para divulgação de revogação
- 4.4.14. Requisitos para verificação de outras formas de divulgação de revogação
- 4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.5. Procedimentos de Auditoria de Segurança

- 4.5.1. Tipos de eventos registrados
- 4.5.2. Frequência de auditoria de registros (*logs*)
- 4.5.3. Período de retenção para registros (*logs*) de auditoria
- 4.5.4. Proteção de registro (*log*) de auditoria
- 4.5.5. Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria
- 4.5.6. Sistema de coleta de dados de auditoria
- 4.5.7. Notificação de agentes causadores de eventos
- 4.5.8. Avaliações de vulnerabilidade

4.6. Arquivamento de Registros

- 4.6.1. Tipos de registros arquivados
- 4.6.2. Período de retenção para arquivo
- 4.6.3. Proteção de arquivo
- 4.6.4. Procedimentos para cópia de segurança (*backup*) de arquivo
- 4.6.5. Requisitos para datação (*time-stamping*) de registros
- 4.6.6. Sistema de coleta de dados de arquivo
- 4.6.7. Procedimentos para obter e verificar informação de arquivo

4.7. Troca de chave

4.8. Comprometimento e Recuperação de Desastre

- 4.8.1. Recursos computacionais, software ou dados são corrompidos
- 4.8.2. Certificado de entidade é revogado
- 4.8.3. Chave de entidade é comprometida
- 4.8.4. Segurança dos recursos após desastre natural ou de outra natureza
- 4.8.5. Atividades das Autoridades de Registro

4.9. Extinção dos serviços de AC, AR ou PSS

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os itens seguintes são referidos aos correspondentes da DPC da AC VALID BRASIL.

5.1. Controles Físicos

- 5.1.1. Construção e localização das instalações da AC VALID BRASIL
- 5.1.2. Acesso físico nas instalações da AC VALID BRASIL
- 5.1.3. Energia e ar condicionado nas instalações da AC VALID BRASIL
- 5.1.4. Exposição à água nas instalações da AC VALID BRASIL
- 5.1.5. Prevenção e proteção contra incêndio nas instalações da AC VALID BRASIL
- 5.1.6. Armazenamento de mídia nas instalações da AC VALID BRASIL
- 5.1.7. Destruição de lixo nas instalações da AC VALID BRASIL
- 5.1.8. Instalações de segurança (*backup*) externas (*off-site*) para AC VALID BRASIL

5.2. Controles Procedimentais

- 5.2.1. Perfis qualificados
- 5.2.2. Número de pessoas necessário por tarefa
- 5.2.3. Identificação e autenticação para cada perfil

5.3. Controles de Pessoal

- 5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade
- 5.3.2. Procedimentos de verificação de antecedentes
- 5.3.3. Requisitos de treinamento
- 5.3.4. Frequência e requisitos para reciclagem técnica
- 5.3.5. Frequência e sequência de rodízio de cargos
- 5.3.6. Sanções para ações não autorizadas
- 5.3.7. Requisitos para contratação de pessoal
- 5.3.8. Documentação fornecida ao pessoal

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, nesta PC são definidas medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC A3 da AC VALID BRASIL. Também são definidos outros controles técnicos de segurança utilizados pela AC VALID BRASIL e pelas ARs vinculadas na execução de suas funções operacionais.

6.1. Geração e Instalação do Par de Chaves

Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, publicando nova versão do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

6.1.1. Geração do par de chaves

6.1.1.1. Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is) a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1. Não se aplica.

6.1.1.1.2. Não se aplica.

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (*Cryptographic Service Provider*) existente na estação do solicitante apresentados pelo browser . A geração do par de chaves criptográficas ocorre utilizando hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

6.1.1.4. Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL. As chaves privadas correspondentes aos certificados deverão ser armazenadas em *hardware* criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO e com capacidade de geração de chave, sendo ativados e protegidos por senha e/ou identificação biométrica, definido para o tipo de certificado A3.

6.1.1.5. A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

6.1.1.6. A mídia de armazenamento da chave privada assegura por meios técnicos e procedimentais adequados, no mínimo, que:

- a) a chave privada é única e seu sigilo é suficientemente assegurado;
- b) a chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7. Essa mídia de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica
---------------------	---

(Requisitos Mínimos)	
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

Nota: A responsabilidade pela segurança na garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do titular ou responsável pelo uso do certificado, conforme especificado no Termo de Titularidade.

6.1.2. Entrega da chave privada à entidade titular

Não se aplica.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC VALID BRASIL por meio de uma troca *online* utilizando funções automáticas do software de certificação da AC VALID BRASIL. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital, realizada com a chave privada correspondente à chave pública contida na solicitação. Procedimentos de orientação contidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

6.1.4. Disponibilização de chave pública da AC VALID BRASIL para usuários

A AC VALID BRASIL disponibiliza todos os certificados da sua cadeia de certificação para os usuários da ICP-Brasil, nas seguintes formas:

- a) no momento da disponibilização de um certificado para seu titular; usando formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2];
- b) diretório;
- c) página web da AC VALID BRASIL (<https://www.validcertificadora.com.br/index.aspx?DID=301>); e
- d) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Nesta PC, os certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V2 e V5 tem o tamanho admitido para chaves criptográficas de titular final de 2048 bits.

6.1.5.2. Os algoritmos e o tamanhos de chaves a serem utilizados nos certificados tipo A3 da ICP-Brasil, estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [2].

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas das entidades titulares de certificados são o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

6.1.8. Geração de chave por *hardware* ou *software*

A geração das chaves criptográficas do Certificado tipo A3 desta PC é realizada em *hardware criptográfico*, previsto pela ICP-Brasil.

6.1.9. Propósitos de uso de chave (conforme o campo “*key usage*” na X.509 v3)

As chaves privadas dos Titulares de Certificados emitidos pela AC VALID BRASIL serão utilizadas para as aplicações descritas no item 1.3.5. Para tanto, os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

6.2. Proteção da Chave Privada

Neste item são definidos os requisitos de proteção das chaves privadas de certificados emitidos, segundo a PC A3 da AC VALID BRASIL.

6.2.1. Padrões para módulo criptográfico

Não se aplica.

6.2.2. Controle “n de m” para chave privada

Não se aplica.

6.2.3. Custódia (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a custódia (*escrow*) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. Cópia de segurança (*backup*) de chave privada

6.2.4.1. O titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC VALID BRASIL não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC VALID BRASIL poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.

6.2.4.3. Em qualquer caso, a cópia de segurança armazenada será cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [2] e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. Não se aplica.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC VALID BRASIL não arquivava cópias de chaves privadas de assinatura digital de titulares de certificados.

6.2.5.2. Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6. Inserção de chave privada em módulo criptográfico

Os Titulares de Certificados poderão optar por utilizar um *hardware* criptográfico para armazenar sua chave privada após a aceitação do certificado.

6.2.7. Método de ativação de chave privada

O titular do certificado pode definir procedimentos necessários para a ativação de sua chave privada. Recomenda-se que a chave privada seja protegida por senha e que para sua ativação seja solicitada essa senha, que deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo.

6.2.8. Método de desativação de chave privada

Cada entidade titular de certificado pode definir os procedimentos necessários para a desativação da sua chave privada.

6.2.9. Método de destruição de chave privada

Cada entidade titular de certificado pode definir os procedimentos necessários para a destruição da sua chave privada.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas de titulares dos certificados de assinatura digital e as LCRs são armazenadas pela AC VALID BRASIL, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos respectivos titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. O período máximo de validade admitido para certificados de assinatura digital tipo A3 da AC VALID BRASIL é de até 5 (cinco) anos, previsto pela ICP-Brasil.

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

Para certificados do tipo A3, a geração e armazenamento do par de chaves são realizados em *hardware* criptográfico (*cartão inteligente ou token*), com capacidade de geração de chave, sendo ativado e protegido por senha e/ou identificação biométrica.

6.4.2. Proteção dos dados de ativação

No caso da ativação por senhas, recomenda-se que elas sejam criadas e cadastradas de forma aleatória, com procedimentos básicos de segurança:

- a) nunca fornecer senha a terceiros;
- b) escolher senhas de 8 ou mais caracteres;
- c) definir senhas com caracteres numéricos e alfanuméricos;
- d) memorizar a senha; e
- e) não escrevê-la (se necessário, guardar em local com segurança, sem acesso de terceiros).

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. A geração do par de chaves sempre deverá ocorrer no equipamento do solicitante do certificado digital, é de responsabilidade do cliente ter disponível recursos computacionais necessários para prover a segurança e integridade da chave privada relacionada ao seu certificado digital, no momento da emissão.

Recomenda-se que as chaves privadas sejam protegidas por senha e que os equipamentos onde são geradas e utilizadas disponham de mecanismos mínimos de segurança computacional, tais como:

- a) Senha de *bios* ativada;
- b) Controle de acesso lógico ao sistema operacional;
- c) Exigência de uso de senhas fortes;
- d) Diretivas de senha e de bloqueio de conta;
- e) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;
- f) *Firewall* pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- g) Sistema operacional atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc);
- h) Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2. Classificação da segurança computacional

Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

Não se aplica.

6.6.1. Controles de desenvolvimento de sistema

Não se aplica.

6.6.2. Controles de gerenciamento de segurança

Não se aplica.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.7. Controles de Segurança de Rede

Não se aplica.

6.8. Controles de Engenharia do Módulo Criptográfico

Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado obedecem aos padrões de referência definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

7. PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCR gerados segundo esta PC. São informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são obrigatoriamente atendidos pelo tipo de certificado admitido (A3), no âmbito da ICP-Brasil.

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC VALID BRASIL, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1. Número de versão

Todos os certificados emitidos pela AC VALID BRASIL, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2. Extensões de certificado

7.1.2.1. Neste item, esta PC descreve todas as extensões de certificado utilizadas pela AC VALID BRASIL e sua criticalidade.

7.1.2.2. A ICP-Brasil define as seguintes extensões obrigatórias:

a) "**Authority Key Identifier**", **não crítica**: o campo keyIdentifier contém o *hash* SHA-1 da chave pública da AC VALID BRASIL;

b) "**Key Usage**", **crítica**: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;

c) "**Certificate Policies**", **não crítica**: contém:

c.1) o OID desta PC: 2.16.76.1.2.3.35; e

c.2) o endereço Web da DPC da AC VALID BRASIL:

<https://www.validcertificadora.com.br/index.aspx?DID=301>.

d) "**CRL Distribution Points**", **não crítica**: contém os endereços na Web onde se obtém a LCR correspondente;

Para certificados digitais emitidos na cadeia V2:

d.1) <http://icp-brasil.validcertificadora.com.br/ac-validbrasil/lcr-ac-validbrasilv2.crl>

d.2) <http://icp-brasil2.validcertificadora.com.br/ac-validbrasil/lcr-ac-validbrasil2.crl>

d.3) <http://repositorio.icpbrasil.gov.br/lcr/VALID/lcr-ac-validbrasilv2.crl>

Para certificados digitais emitidos da cadeia V5:

d.4) <http://icp-brasil.validcertificadora.com.br/ac-validbrasil/lcr-ac-validbrasilv5.crl>

d.5) <http://icp-brasil2.validcertificadora.com.br/ac-validbrasil/lcr-ac-validbrasilv5.crl>

e) "**Authority Information Access**", **não crítica**: A primeira entrada contém o método de acesso id-ad-calssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação.

Para certificados digitais emitidos na cadeia V2:

<http://icp-brasil.validcertificadora.com.br/ac-validbrasil/ac-validbrasilv2.p7b>

Para certificados digitais emitidos na cadeia V5:

<http://icp-brasil.validcertificadora.com.br/ac-validbrasil/ac-validbrasilv5.p7b>

A entrada contém o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, utilizando um dos seguintes protocolos de acesso HTTP, nos seguintes endereços, onde estas extensões somente são aplicáveis para certificados de usuário final.

Para certificados digitais emitidos na cadeia V2:

<http://ocsp.validcertificadora.com.br>

Para certificados digitais emitidos na cadeia V5:

<http://ocspv5.validcertificadora.com.br>

f) "**basicConstraints**", **não crítica**: contém o campo cA=False.

7.1.2.3. A AC VALID BRASIL implementa nos certificados emitidos segundo esta PC a extensão "**Subject Alternative Name**", **não crítica**, definida pela ICP-Brasil como obrigatória, com os seguintes formatos:

a) Para certificado de pessoa física:

a.1) 3 (três) campos otherName, obrigatórios, contendo:

- i. **OID = 2.16.76.1.3.1 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

- ii. **OID = 2.16.76.1.3.6 e conteúdo** = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI), Cadastro de Atividade Econômica da Pessoa Física (CAEPF) ou Cadastro Nacional de Obras (CNO) da pessoa física titular do certificado.
 - iii. **OID = 2.16.76.1.3.5 e conteúdo** = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor;
- a.2) Não se aplica.
 - a.3) Não se aplica.
 - a.4) Não se aplica.

b) Para certificado de pessoa jurídica:

4 (quatro) campos otherName, obrigatórios, contendo nesta ordem:

- i. **OID = 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato *ddmmaaaa*; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF;
 - ii. **OID = 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;
 - iii. **OID = 2.16.76.1.3.3 e conteúdo** = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;
 - iv. **OID = 2.16.76.1.3.7 e conteúdo** = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI), Cadastro de Atividade Econômica da Pessoa Física (CAEPF) ou Cadastro Nacional de Obras (CNO) da pessoa jurídica titular do certificado;
- c) Não se aplica.
 - d) Não se aplica.
 - e) Não se aplica.

7.1.2.4. Os campos otherName, definidos como obrigatórios pela ICP-Brasil, estão de acordo com as seguintes especificações:

- a) O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;

- b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI/CAEPF/CNO, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
- c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;
- d) Quando a identificação profissional não estiver disponível, não será inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;
- e) Todas informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;
- f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;
- g) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;
- h) Não se aplica.
- i) h) O campo UPN é opcional, caso não seja usado o OID não é incluído no certificado.

7.1.2.5. Campos `otherName` adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC VALID BRASIL, podem ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

7.1.2.6. Os outros campos que compõem a extensão "Subject Alternative Name" poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.7. Não se aplica.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC VALID BRASIL são assinados com o uso do algoritmo RSA com SHA-256 como função de *hash* (OID = 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função *hash* (OID = 1.2.840.113549.1.1.13), conforme o padrão PKCS#1, observados os algoritmos admitidos no âmbito da ICP-Brasil, documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

7.1.4. Formatos de nome

7.1.4.1. O nome do titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR;

O = ICP-Brasil;

OU = empresa associada ao emissor do certificado, intermediando o fornecimento de certificados;

OU = nome fantasia (nome que associa uma entidade ao certificado);

OU = unidade (identifica grupo, área, divisão, seção ou qualquer outra identificação semelhante);

OU = referência (indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou sequência alfanumérica);

OU = código (número, nome ou sequência alfanumérica); **OU** = identificador (sequência alfanumérica);

OU = escopo (finalidade do certificado ou seu domínio de aplicação no contexto de um uso específico);

OU = o CNPJ da AR que realizou a identificação presencial;

CN = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, contém o nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica); em um certificado de equipamento ou aplicação, o identificador CN contém o URL correspondente. No caso do certificado de pessoa jurídica para o sistema COMPE, o formato será CCCC-XXX, onde CCCC=quatro posições numéricas contendo o código da instituição financeira e XXX=Nome da Instituição Financeira.

NOTA 1: Será escrito o nome até o limite do tamanho do campo disponível, vedada à abreviatura.

NOTA 2: Caso qualquer um dos campos OU acima não seja utilizado, o mesmo será grafado com o texto "(EM BRANCO)".

7.1.4.2. Não se aplica.

7.1.5. Restrições de nome

7.1.5.1. Neste item da PC, são descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
branco	20
!	21
“	22
#	23
\$	24
%	25

&	26
'	27
(28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6. OID (*Object Identifier*) de Política de Certificado

O OID (*Object Identifier*) desta PC é 2.16.76.1.2.3.35.

7.1.7. Uso da extensão “Policy Constraints”

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo *policyQualifiers* da extensão “*Certificate Policies*” contém o endereço da página Web (*URL*) com a DPC da AC VALID BRASIL: <http://icp-brasil.validcertificadora.com.br/ac-validbrasil/dpc-ac-validbrasilv5.pdf> .

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número de versão

As LCRs geradas pela AC VALID BRASIL, segundo esta PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC VALID BRASIL e sua criticalidade.

7.2.2.2. As LCRs da AC VALID BRASIL definem as seguintes extensões:

- a) “**Authority Key Identifier**”, **não crítica**: contém o *hash* SHA-1 da chave pública da AC VALID BRASIL que assina a LCR; e
- b) “**CRL Number**”, **não crítica**: contém um número sequencial para cada LCR emitida.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

As alterações nas especificações desta PC são realizadas pela AC VALID BRASIL. Quaisquer modificações são submetidas à aprovação do CG da ICP-Brasil.

8.2. Políticas de publicação e notificação

A AC VALID BRASIL mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web: <https://www.validcertificadora.com.br/Politica-de-Certificado/D323>.

8.3. Procedimentos de aprovação

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC VALID BRASIL, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com o documento citado, será verificada a compatibilidade entre esta PC e a DPC da AC VALID BRASIL. Novas versões serão igualmente submetidas à aprovação do CG da ICP-Brasil.

9. DOCUMENTOS REFERENCIADOS

9.1. Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O site <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

9.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O site <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[2]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

10. LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC - Raiz Autoridade Certificadora Raiz da ICP-Brasil
ACT - Autoridade de Carimbo do Tempo
AR - Autoridades de Registro
CAEPF - Cadastro de Atividade Econômica da Pessoa Física
CEI - Cadastro Específico do INSS
CF-e - Cupom Fiscal Eletrônico
CG - Comitê Gestor
CMM-SEI - Capability Maturity Model do Software Engineering Institute
CMVP - Cryptographic Module Validation Program
CN - Common Name

CNE - Carteira Nacional de Estrangeiro
CNO - Cadastro Nacional de Obras
CNPJ - Cadastro Nacional de Pessoas Jurídicas
COBIT - Control Objectives for Information and related Technology
COSO - Comittee of Sponsoring Organizations
CONFAZ - Conselho Nacional de Política Fazendária
CPF - Cadastro de Pessoas Físicas
DMZ - Zona Desmilitarizada
DN - Distinguished Name
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira
IDS - Intrusion Detection System
IEC - International Electrotechnical Commission
INMETRO - Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO - International Organization for Standardization
ITSEC - European Information Technology Security Evaluation Criteria
ITU - International Telecommunications Union
LCR - Lista de Certificados Revogados
NBR - Norma Brasileira
NIST - National Institute of Standards and Technology
NIS - Número de Identificação Social
OCSP - Online Certificate Status Protocol
OID - Object Identifier
OM-BR - Objetos Metrológicos ICP-Brasil
OU - Organization Unit
PASEP - Programa de Formação do Patrimônio do Servidor Público
PC - Políticas de Certificado
PCN - Plano de Continuidade de Negócio
PIS - Programa de Integração Social
POP - Proof of Possession
PS - Política de Segurança
PSS - Prestadores de Serviço de Suporte
RFC - Request for Comments
RG - Registro Geral
SAT - Sistema de Autenticação e Transmissão
SNMP - Simple Network Management Protocol
TCSEC - Trusted System Evaluation Criteria
TSDM - Trusted Software Development Methodology
UF - Unidade de Federação
URL - Uniform Resource Locator