www.serpro.gov.br

Política de Certificação
da
Autoridade Certificadora
do
SERPRO-JUS

Certificados A1

(PC SERPRO-JUS A1)

Versão 3.0 de 24/10/2011

Serviço Federal de Processamento de Dados SERPRO

Classificação: Ostensivo

Controle de Versão

Versão	Data	Motivo	Descrição
1.0	07/03/2005	Criação	Versão Inicial
2.0	26/06/2006	Alteração	Adequações às Resoluções da ICP-Brasil
2.1	27/04/2009	Alteração	Inclusão dos endereços da LCR (item 7.1.2.2): Adequações para a versão 2.1 do Leiaute dos Certificados definido pela ACJUS (itens 1.3.4, 1.3.5, 7.1.2.2, 7.1.2.3, 7.1.2.4, 7.1.2.6, 7.1.4) Inclusão da extensão AIA ("*Authority Information Access"*) no item 7.1.2.6;
3.0	24/10/2011	Alteração	Atualizações de acordo com DOC-ICP-04 versão 3.2 e criação da ACSERPRO JUS v4 sob a cadeia da AC Raiz v2. Alterados os seguintes itens: 1.1, 1.3.1.1, 1.3.5.5, 1.3.5.6, 1.4, 6.1.1.2, 6.1.4, 6.1.5, 6.8, 7.1, 7.1.1, 7.1.2.2, 7.1.2.4.a, 7.1.2.6, 7.1.3, 7.1.9, 7.2.1, 7.2.2, 8.3.

LISTA DE ACRÔNIMOS 9

1. INTRODUÇÃO 10

1.1. VISÃO GERAL 10
1.2. IDENTIFICAÇÃO 10
1.3. COMUNIDADE E APLICABILIDADE 10
1.3.1. AUTORIDADES CERTIFICADORAS 10
1.3.2. AUTORIDADES DE REGISTRO 11
1.3.3 PRESTADOR DE SERVIÇO DE SUPORTE 11
1.3.4. TITULARES DE CERTIFICADO 11
1.3.5. APLICABILIDADE 12
1.4. DADOS DE CONTATO 12

2. DISPOSIÇÕES GERAIS 13

2.1. OBRIGAÇÕES E DIREITOS 13
2.1.1. OBRIGAÇÕES DA AC 13
2.1.2. OBRIGAÇÕES DAS AR 13
2.1.3. OBRIGAÇÕES DO TITULAR DO CERTIFICADO 13
2.1.4. DIREITOS DA TERCEIRA PARTE (*RELYING PARTY*) 13
2.1.5. OBRIGAÇÕES DO REPOSITÓRIO 13
2.2. RESPONSABILIDADES 13
2.2.1. RESPONSABILIDADES DA AC 13
2.2.2. RESPONSABILIDADES DA AR 13
2.3. RESPONSABILIDADE FINANCEIRA 13
2.3.2. RELAÇÕES FIDUCIÁRIAS 13
2.3.3. PROCESSOS ADMINISTRATIVOS 14
2.4. INTERPRETAÇÃO E EXECUÇÃO 14
2.4.1. LEGISLAÇÃO 14
2.4.2. FORMA DE INTERPRETAÇÃO E NOTIFICAÇÃO 14
2.4.3. PROCEDIMENTOS DE SOLUÇÃO DE DISPUTA 14
2.5. TARIFAS DE SERVIÇO 14
2.5.1. TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS 14
2.5.2. TARIFAS DE ACESSO A CERTIFICADOS 14
2.5.3. TARIFAS DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS 14
2.5.4. TARIFAS PARA OUTROS SERVIÇOS 14
2.5.5. POLÍTICA DE REEMBOLSO 14

2.6. PUBLICAÇÃO E REPOSITÓRIO 14
2.6.1. PUBLICAÇÃO DE INFORMAÇÃO DA AC 14
2.6.2. FREQÜÊNCIA DE PUBLICAÇÃO 14
2.6.3. CONTROLES DE ACESSO 14
2.6.4. REPOSITÓRIOS 14
2.7. AUDITORIA E FISCALIZAÇÃO 14
2.8. SIGILO 14
2.8.1. TIPOS DE INFORMAÇÕES SIGILOSAS 14
2.8.2. TIPOS DE INFORMAÇÕES NÃO SIGILOSAS 14
2.8.3. DIVULGAÇÃO DE INFORMAÇÃO DE REVOGAÇÃO E DE SUSPENSÃO DE CERTIFICADO 14
2.8.4. QUEBRA DE SIGILO POR MOTIVOS LEGAIS 14
2.8.5. INFORMAÇÕES A TERCEIROS 14
2.8.6. DIVULGAÇÃO POR SOLICITAÇÃO DO TITULAR 14
2.8.7. OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO 15
2.9. DIREITOS DE PROPRIEDADE INTELECTUAL 15

3. IDENTIFICAÇÃO E AUTENTICAÇÃO 15

3.1. REGISTRO INICIAL 15
3.1.1. DISPOSIÇÕES GERAIS 15
3.1.2. TIPOS DE NOMES 15
3.1.3. NECESSIDADE DE NOMES SIGNIFICATIVOS 15
3.1.4. REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES 15
3.1.5. UNICIDADE DE NOMES 15
3.1.6. PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES 15
3.1.7. RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS 15
3.1.8. MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA 15
3.1.9. AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO 15
3.1.9.1. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO 15
3.1.9.2. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO 15
3.1.10. AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO 15
3.1.10.1. DISPOSIÇÕES GERAIS 15
3.1.10.2. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO 15
3.1.10.3. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO 15
3.1.11. AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO OU APLICAÇÃO 15
3.1.11.1. DISPOSIÇÕES GERAIS 15
3.1.11.2. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO OU APLICAÇÃO 15
3.1.11.3 - INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO OU APLICAÇÃO 15
3.2. GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL 16
3.3. GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO 16
3.4. SOLICITAÇÃO DE REVOGAÇÃO 16

4. REQUISITOS OPERACIONAIS 16

4.1. SOLICITAÇÃO DE CERTIFICADO 16
4.2. EMISSÃO DE CERTIFICADO 16
4.3. ACEITAÇÃO DE CERTIFICADO 16
4.4. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO 16
4.4.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO 16
4.4.2. QUEM PODE SOLICITAR REVOGAÇÃO 16
4.4.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO 16
4.4.4. PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO 16
4.4.5. CIRCUNSTÂNCIAS PARA SUSPENSÃO 16
4.4.6. QUEM PODE SOLICITAR SUSPENSÃO 16
4.4.7. PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO 16
4.4.8. LIMITES NO PERÍODO DE SUSPENSÃO 16
4.4.9. FREQÜÊNCIA DE EMISSÃO DE LCR 16
4.4.10. REQUISITOS PARA VERIFICAÇÃO DE LCR 16
4.4.11. DISPONIBILIDADE PARA REVOGAÇÃO OU VERIFICAÇÃO DE STATUS *ON-LINE* 16
4.4.12. REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO *ON-LINE* 16
4.4.13. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO 16
4.4.14. REQUISITOS PARA VERIFICAÇÃO DE OUTRAS FORMAS DE DIVULGAÇÃO DE REVOGAÇÃO 16
4.4.15. REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE 17
4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA 17
4.5.1. TIPOS DE EVENTOS REGISTRADOS 17
4.5.2. FREQÜÊNCIA DE AUDITORIA DE REGISTROS (*LOGS*) 17
4.5.3. PERÍODO DE RETENÇÃO PARA REGISTROS (*LOGS*) DE AUDITORIA 17
4.5.4. PROTEÇÃO DE REGISTRO (*LOG*) DE AUDITORIA 17
4.5.5. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (*BACKUP*) DE REGISTRO (*LOG*) DE AUDITORIA 17
4.5.6. SISTEMA DE COLETA DE DADOS DE AUDITORIA 17
4.5.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS 17
4.5.8. AVALIAÇÕES DE VULNERABILIDADE 17
4.6. ARQUIVAMENTO DE REGISTROS 17
4.6.1. TIPOS DE REGISTROS ARQUIVADOS 17
4.6.2. PERÍODO DE RETENÇÃO PARA ARQUIVO 17
4.6.3. PROTEÇÃO DE ARQUIVO 17
4.6.4. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (*BACKUP*) DE ARQUIVO 17
4.6.5. REQUISITOS PARA DATAÇÃO (*TIME-STAMPING*) DE REGISTROS 17
4.6.6. SISTEMA DE COLETA DE DADOS DE ARQUIVO 17
4.6.7. PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO 17
4.7. TROCA DE CHAVE 17
4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE 17
4.8.1. RECURSOS COMPUTACIONAIS, SOFTWARE OU DADOS SÃO CORROMPIDOS 18
4.8.2. CERTIFICADO DE ENTIDADE É REVOGADO 18

4.8.3. CHAVE DE ENTIDADE É COMPROMETIDA 18
4.8.4. SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA NATUREZA 18
4.8.5. ATIVIDADES DAS AUTORIDADES DE REGISTRO 18
4.9. EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS 18

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL 18

5.1. CONTROLES FÍSICOS 18
5.1.1. CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES 18
5.1.2. ACESSO FÍSICO 18
5.1.3. ENERGIA E AR CONDICIONADO 18
5.1.4. EXPOSIÇÃO À ÁGUA 18
5.1.5. PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO 18
5.1.6. ARMAZENAMENTO DE MÍDIA 18
5.1.7. DESTRUIÇÃO DE LIXO 18
5.1.8. INSTALAÇÕES DE SEGURANÇA (*BACKUP*) EXTERNAS (*OFF-SITE*) 18
5.2. CONTROLES PROCEDIMENTAIS 18
5.2.1. PERFIS QUALIFICADOS 18
5.2.2. NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA 18
5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL 18
5.3. CONTROLES DE PESSOAL 18
5.3.1. ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE 18
5.3.2. PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES 19
5.3.3. REQUISITOS DE TREINAMENTO 19
5.3.4. FREQÜÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA 19
5.3.5. FREQÜÊNCIA E SEQÜÊNCIA DE RODÍZIO DE CARGOS 19
5.3.6. SANÇÕES PARA AÇÕES NÃO AUTORIZADAS 19
5.3.7. REQUISITOS PARA CONTRATAÇÃO DE PESSOAL 19
5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL 19

6. CONTROLES TÉCNICOS DE SEGURANÇA 19

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES 19
6.1.1. GERAÇÃO DO PAR DE CHAVES 19
6.1.2. ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR 20
6.1.3. ENTREGA DA CHAVE PÚBLICA PARA O EMISSOR DE CERTIFICADO 20
6.1.4. DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC PARA USUÁRIOS 20
6.1.5. TAMANHOS DE CHAVE 21
6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS 21
6.1.7 VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS 21
6.1.8 GERAÇÃO DE CHAVE POR *HARDWARE OU SOFTWARE* 21
6.1.9. PROPÓSITOS DE USO DE CHAVE (CONFORME O CAMPO "*KEY USAGE*" NA X.509 V3) 21
6.2. PROTEÇÃO DA CHAVE PRIVADA 21

6.2.1. PADRÕES PARA MÓDULO CRIPTOGRÁFICO 21
6.2.2. CONTROLE "N DE M" PARA CHAVE PRIVADA 22
6.2.3. CUSTÓDIA (*ESCROW*) DE CHAVE PRIVADA 22
6.2.4. CÓPIA DE SEGURANÇA (*BACKUP*) DE CHAVE PRIVADA 22
6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA 22
6.2.6 INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO 22
6.2.7. MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA 22
6.2.8. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA 22
6.2.9 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA 23
6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES 23
6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA 23
6.3.2 PERÍODOS DE USO PARA AS CHAVES PÚBLICA E PRIVADA 23
6.4 DADOS DE ATIVAÇÃO 23
6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO 23
6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO 23
6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL 23
6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL 23
6.5.2 CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL 24
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA 24
6.6.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA 24
6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA 24
6.6.3 CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA 24
6.6.4 CONTROLES NA GERAÇÃO DA LCR ANTES DE PUBLICADAS 24
6.7. CONTROLES DE SEGURANÇA DE REDE 24
6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO 24

7. PERFIS DE CERTIFICADO E LCR 24

7.1 PERFIL DO CERTIFICADO 24
7.1.1 NÚMERO DE VERSÃO 25
7.1.2 EXTENSÕES DE CERTIFICADO 25
7.1.3 IDENTIFICADORES DE ALGORITMO 27
7.1.4 FORMATOS DE NOME 27
7.1.5. RESTRIÇÕES DE NOME 29
7.1.6 OID (*OBJECT IDENTIFIER*) DE POLÍTICA DE CERTIFICADO 30
7.1.7 USO DA EXTENSÃO *"POLICY CONSTRAINTS"* 30
7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA 30
7.1.9. SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS 30
7.2. PERFIL DE LCR 30
7.2.1. NÚMERO DE VERSÃO 30
7.2.2 EXTENSÕES DE LCR E DE SUAS ENTRADAS 30

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO 31

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO 31
8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO 31
8.3 PROCEDIMENTOS DE APROVAÇÃO 31

9. DOCUMENTOS REFERENCIADOS 31

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
AR - Autoridades de Registro
CEI - Cadastro Específico do INSS
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
CNPJ - Cadastro Nacional de Pessoas Jurídicas -
COBIT - *Control Objectives for Information and related Technology*
COSO - *Comitee of Sponsoring Organizations*
CPF - Cadastro de Pessoas Físicas
DMZ - Zona Desmilitarizada
DN - *Distinguished Name*
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira
IDS - Sistemas de Detecção de Intrusão
IEC - *International Electrotechnical Commission*
ISO – *International Organization for Standardization*
ITSEC - *European Information Technology Security Evaluation Criteria*
ITU - *International Telecommunications Union*
LCR - Lista de Certificados Revogados
NBR - Norma Brasileira
NIS - Número de Identificação Social
NIST - *National Institute of Standards and Technology*
OCSP - *On-line Certificate Status Protocol*
OID - *Object Identifier*
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*
PSS - Prestadores de Serviço de Suporte
RFC – *Request For Comments*
RG - Registro Geral
SNMP - *Simple Network Management Protocol*
TCSEC - *Trusted System Evaluation Criteria*
TSDM - *Trusted Software Development Methodology*
UF - Unidade de Federação
URL - Uniform Resource Location

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Este documento estabelece os requisitos a serem obrigatoriamente observados pela AC SERPRO-JUS integrante da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2 A PC AC SERPRO-JUS A1 elaborada no âmbito da ICP-Brasil adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04).

1.1.3 O tipo de certificado emitido sob esta PC é o Tipo A1.

1.1.4 Os tipos de certificados de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

1.1.5 Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6 Item não aplicável.

1.1.7 Outros tipos de certificado podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescidas aos tipos de certificados aceitos pela ICP-Brasil.

1.2. IDENTIFICAÇÃO

1.2.1 Esta PC obedece às recomendações da ICP-Brasil para a emissão de certificados de assinatura do tipo A1.

1.2.2 Após o processo de credenciamento da AC SERPRO-JUS foi atribuído a esta Política de Certificação no âmbito da ICP-Brasil o seguinte OID;

TIPO DE CERTIFICADO	OID
A1	2.16.76.1.2.1.21

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. Autoridades Certificadoras

1.3.1.1 A Autoridade Certificadora do SERPRO-JUS (AC SERPRO-JUS) integra a Infra-estrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora do SERPRO-JUS (AC SERPRO-JUS) e da Autoridade Certificadora Raiz Brasileira.

1.3.1.2 Esta PC é implementada pela Autoridade Certificadora SERPRO-JUS cuja DPC (DPC da AC SERPRO-JUS) encontra-se publicada na página *Web* da mesma, conforme item 2.6.1.

1.3.2. Autoridades de Registro

1.3.2.1 A AC SERPRO-JUS mantém página web (https://ccd.serpro.gov.br/acserprojus) onde estão publicados os seguintes dados, referentes às Autoridades de Registro - AR utilizadas pela AC SERPRO-JUS 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 AR credenciadas, com informações sobre as PC 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, 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 AR vinculadas com outras AR da ICP-Brasil, se for caso.

1.3.2.2 A AC SERPRO-JUS mantém as informações acima sempre atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A AC SERPRO-JUS não utiliza prestador de serviço de suporte em suas operações;
1.3.3.2 PSS são entidades utilizadas pela AC ou pela AR para desempenhar as atividades descritas abaixo:
a) disponibilização de infra-estrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.
1.3.3.3 A AC SERPRO-JUS mantém as informações acima atualizadas.

1.3.4. Titulares de Certificado

Os certificados Cert-JUS identificam seus titulares relacionando-os a um determinado órgão público. Cada órgão público que desejar fazer uso de certificados Cert-JUS deverá responsabilizar-se pelas informações funcionais e institucionais constantes na **AUTORIZAÇÃO** e no certificado.

1.3.4.1 Os certificados Cert-JUS destinam-se aos órgãos da administração pública direta e indireta.
1.3.4.2 Órgãos **não pertencentes** ao Poder Judiciário deverão solicitar

CADASTRAMENTO junto à AC-JUS, para a emissão de certificados Cert-JUS.

1.3.4.2.1 A AC SERPRO-JUS somente emitirá certificados para órgãos **não pertencentes** ao Poder Judiciário cujo **CADASTRAMENTO** tenha sido aprovado pela **AC-JUS**.

1.3.4.2.2 Para emissão de certificados Cert-JUS para órgãos do **Poder Judiciário** não é necessário **CADASTRAMENTO** prévio na **AC-JUS**

1.3.4.3 Para a emissão de qualquer certificado Cert-JUS é necessária **AUTORIZAÇÃO** da **autoridade competente** da instituição à qual o certificado está relacionado.

1.3.4.3.1 Para o disposto neste documento, entende-se como **autoridade competente:**

a) a autoridade máxima do órgão;
b) o representante legal do órgão;
c) outra pessoa expressamente designada para esta finalidade, por meio de documento oficial.

1.3.4.4 O titular do Cert-JUS **Equipamento Servidor** será sempre um órgão público e o responsável pelo certificado deverá ser, obrigatoriamente, servidor público, indicado e autorizado pela autoridade competente.

1.3.4.5 O titular do Cert-JUS **Código Seguro** será sempre um órgão do **Poder Judiciário ou órgão da administração pública direta e indireta** e o responsável pelo certificado deverá ser, obrigatoriamente, servidor público, indicado e autorizado pela autoridade competente.

1.3.5. Aplicabilidade

1.3.5.1 Certificados Cert-JUS **Equipamento Servidor:**

1.3.5.1.1 Os certificados digitais Cert-JUS **Equipamento Servidor** destinam-se **exclusivamente** para utilização em equipamentos que disponibilizem serviços ou informações do poder público, tais como web segura, SSH, e outros serviços que requeiram certificados digitais para autenticação de servidor.

1.3.5.1.2 Destina-se também a equipamentos que ofereçam serviços como **Carimbo de Tempo (timestamping), OCSP, ou outras aprovadas pela ICP-Brasil**.

1.3.5.1.3 Os certificados Cert-JUS **Equipamento Servidor** devem ser utilizados somente em equipamentos servidores pertencentes a órgão do **Poder Judiciário, órgãos da administração pública direta e indireta** ou a empresas privadas que prestem serviços a órgãos públicos.

1.3.5.2 Certificados Cert-JUS **Código Seguro:**

1.3.5.2.1 O certificado Cert-JUS **Código Seguro** destina-se, exclusivamente, para assinatura de código de software, desenvolvido, disponibilizado ou contratado por órgão do **Poder Judiciário e órgãos da administração pública direta e indireta**,

1.3.5.3 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 por qualquer AC credenciada pela AC Raiz.

1.3.5.4 Certificados de tipo A1 são 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.

1.4. DADOS DE CONTATO

Esta PC é administrada pelo Centro de Certificação Digital do SERPRO, CCD-SERPRO, localizado no seguinte endereço:

SGAN 601 Módulo V
Bairro: Asa Norte
CEP: 70.836-900
Brasília / DF.

Pessoas de Contato.

Nome: Gilberto de Oliveira Netto
Telefone: (61) 2021-8651
Fax: (61) 2021-8516
(encaminhar aos cuidados da SUPOP/OPCDI)

E-mail de Contato.

ccdserpro@serpro.gov.br

2. DISPOSIÇÕES GERAIS

Os itens seguintes estão descritos da DPC AC SERPRO-JUS.

2.1. OBRIGAÇÕES E DIREITOS

2.1.1. Obrigações da AC

2.1.2. Obrigações das AR

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

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

2.6.2. Freqüência 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 estão descritos da DPC AC SERPRO-JUS.

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

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.10. Autenticação da identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.2. Documentos para efeitos de identificação de uma organização

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Disposições Gerais

3.1.11.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.1.11.3 - Informações contidas no certificado emitido para um 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 estão descritos da DPC AC SERPRO-JUS.

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. Freqüência 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. Freqüência 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 estão descritos da DPC AC SERPRO-JUS.

5.1. CONTROLES FÍSICOS

5.1.1. Construção e localização das instalações

5.1.2. Acesso físico

5.1.3. Energia e ar condicionado

5.1.4. Exposição à água

5.1.5. Prevenção e proteção contra incêndio

5.1.6. Armazenamento de mídia

5.1.7. Destruição de lixo

5.1.8. Instalações de segurança (*backup*) externas (*off-site*)

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. Freqüência e requisitos para reciclagem técnica

5.3.5. Freqüência e seqüência 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, são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC AC SERPRO-JUS.

São definidos também outros controles técnicos de segurança utilizados pela AC SERPRO-JUS e pelas AR vinculadas na execução de suas funções operacionais.

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

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.

6.1.1.2 O Titular do Certificado gera a chave utilizando o CSP (Cryptographic Service Provider) existente na estação do solicitante, apresentado pelo browser utilizado e, quando da geração, a chave privada é armazenada no HD da estação. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficos e pelo uso do certificado.

A chave privada é armazenada utilizando o seguinte dispositivo:

HD.
Para certificados de código seguro, na solicitação do certificado pelo Internet Explorer deve ser definido o nível de segurança do repositório como alto. Nos demais browsers, também deve ser definida senha de proteção à chave privada. A chave privada deve ser exportada e armazenada (cópia de segurança) em CD ou outra mídia externa, evitando assim perda do certificado caso a estação do usuário precise ser formatada. A segurança da chave privada repousa, nesse caso, na proteção da

mídia e da senha de acesso à cópia de segurança, e na proteção da senha de acesso à chave privada armazenada no HD.

A ACSERPRO-JUS recomenda ao Titular do Certificado a remoção do certificado do browser de sua estação, após sua utilização, caso o equipamento seja compartilhado com outros usuários.

Para certificados de equipamentos, a proteção da chave privada está na proteção da senha de logon do usuário responsável pelo serviço.

6.1.1.2 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.3 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL[1], no meio de armazenamento definido para cada tipo de certificado A1 previsto pela ICP-Brasil.

6.1.1.4 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.

6.1.1.5 A mídia de armazenamento da chave privada deverá assegurar, 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.

6.1.1.6 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.

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC SERPRO-JUS por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC SERPRO-JUS.
A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4. Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da ACSERPRO-JUS, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1];
b) Página *web* da ACSERPRO-JUS (https://ccd.serpro.gov.br/acserprojus);
c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1 Os tamanhos das chaves criptográficas associadas aos certificados emitidos pela ACSERPRO-JUS são os seguintes:

6.1.5.1.1 Para os certificados emitidos pela ACSERPRO-JUS v4 o tamanho das chaves criptográficas é de, no mínimo, 2048 (dois mil e quarenta e oito) bits;

6.1.5.1.2 Para os certificados emitidos pela ACSERPRO-JUS v3 e ACSERPRO-JUS v1 o tamanho das chaves criptográficas é de 1024 (mil e vinte e quatro) bits.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos Titulares de certificado, adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7 Verificação da qualidade dos parâmetros

Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.8 Geração de chave por *hardware ou software*

O processo de geração do par de chaves dos Titulares do Certificado é feito por software.

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 SERPRO-JUS serão utilizadas conforme descrito no item 1.3.5.

6.2. PROTEÇÃO DA CHAVE PRIVADA

Neste item são definidos os requisitos de proteção das chave privadas de certificados emitidos, segundo a PC AC SERPRO-JUS.

6.2.1. Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que, os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1], são observados para geração das chaves criptográficas.

6.2.2. Controle “n de m” para chave privada

Item não aplicável.

6.2.3. Custódia (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*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 Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.
6.2.4.2 A AC SERPRO-JUS responsável pela PC não mantém cópia de segurança de chave privada de titular.
6.2.4.3 A cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.
6.2.4.4 A cópia de segurança deverá ser protegida por “senha”.

6.2.5 Arquivamento de chave privada

6.2.5.1 Item não aplicável, uma vez que a ICP-Brasil não admite o arquivamento de chaves privadas de assinatura digital.
6.2.5.2 Defini-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, cartão inteligente ou token, para armazenar sua chave privada após a aceitação do certificado.

6.2.7. Método de ativação de chave privada

A chave privada é ativada, mediante senha solicitada pelo software de proteção da chave privada. A senha deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo.

O Titular de certificado deverá adotar senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 3 meses.

6.2.8. Método de desativação de chave privada

A desativação da chave privada ocorre no fechamento do “browser” utilizado para estabelecer uma conexão segura.

6.2.9 Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado deve ser feita através de opções disponibilizadas pelo "browser" utilizado para gerar o par de chaves, a opção permite apagar a chave privada.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A AC SERPRO-JUS prevê que as chaves públicas de titulares dos certificados de assinatura digital e as LCR serão armazenadas pela AC SERPRO-JUS, 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 Certificados do tipo A1 previstos nesta PC tem validade de até 1 ano.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Item não aplicável.

6.4.2 Proteção dos dados de ativação

Item não aplicável.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

Os equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados devem dispor de mecanismos mínimos que garantam a segurança computacional, como, proteção do equipamento com senha e software de CSP para a geração das chaves.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6. Controles Técnicos do Ciclo de Vida

Item não aplicável.

6.6.1. Controles de desenvolvimento de sistema

Item não aplicável.

6.6.2 Controles de gerenciamento de segurança

Item não aplicável.

6.6.3 Classificações de segurança de ciclo de vida

Item não aplicável.

6.6.4 Controles na geração da LCR antes de publicadas

Item não aplicável.

6.7. Controles de Segurança de Rede

Item não aplicável.

6.8 Controles de Engenharia do Módulo Criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (Federal Information Processing Standards) 140-1 – requerido pela AC SERPRO-JUS para os certificados emitidos sob esta PC. Poderão ser indicados padrões de referência, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

7. PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCR gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1 Perfil do Certificado

Todos os certificados emitidos pela ACSERPRO-JUS, 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 SERPRO-JUS, 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, a PC descreve todas as extensões de certificados utilizadas e sua criticalidade.

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

a) "*Authority Key Identifier*", não crítica: o campo **keyIdentifier** contém o resumo SHA-1 da chave pública da ACSERPRO-JUS;

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

c) "*Certificate Policies*", não crítica: o campo ***policyIdentifier*** contém o OID desta PC e o campo ***policyQualifiers*** contém o endereço *URL* da página *Web* *https://ccd.serpro.gov.br/acserprojus/docs/dpcacserprojus.pdf* da ACSERPRO-JUS com a DPC da ACSERPRO-JUS;

d) "**CRL Distribution Points", não crítica**: contém o endereço URL da página Web onde se obtém a LCR da ACSERPRO-JUS:
   - Para os certificados emitidos pela ACSERPRO-JUS v4: *http://ccd.serpro.gov.br/lcr/acserprojusv4.crl*, *http://ccd2.serpro.gov.br/lcr/acserprojusv4.crl* e *http://repositorio.icpbrasil.gov.br/lcr/serpro/acserprojusv4.crl*
   - Para os certificados emitidos pela ACSERPRO-JUS v3: *http://ccd.serpro.gov.br/lcr/acserprojusv3.crl*, *http://ccd2.serpro.gov.br/lcr/acserprojusv3.crl* e *http://www.iti.gov.br/serpro/acserprojusv3.crl*
   - Para os certificados emitidos pela ACSERPRO-JUS v1: *http://ccd.serpro.gov.br/lcr/acserprojus.crl*.

a) não se aplica;

b) **"*Authority Information Access*", não critica**, contendo o método de acesso **id-ad-caIssuer**, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação no seguinte endereço:
   - Para os certificados emitidos pela ACSERPRO-JUS v4: http://ccd.serpro.gov.br/cadeias/acserprojusv4.p7b
   - Para os certificados emitidos pela ACSERPRO-JUS v3: http://ccd.serpro.gov.br/cadeias/acserprojus.p7b
   - OID = 1.3.6.1.5.5.7.1.1.

7.1.2.3. A ICP-Brasil também define como obrigatória a extensão **"Subject Alternative Name"**, **não crítica**, e com os seguintes formatos:

a) Para **certificados** Cert-JUS **Equipamento Servidor** e Cert-JUS **Código Seguro**:

Quatro campos otherName, obrigatórios, contendo:

i. **OID = 2.16.76.1.3.8 e conteúdo =** nome empresarial constante no CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica.
ii. **OID = 2.16.76.1.3.3 e conteúdo** = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;
iii. **OID = 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;
iv. **OID = 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11(onze) posições subseqüentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;

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

a) 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) O preenchimento dos campos: *nome empresarial constante do CNPJ, número do CNPJ, nome, CPF e data de nascimento do responsável pelo certificado*, **é obrigatório**.
c) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
d) 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;
e) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;
f) 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;
g) As 6 (seis) 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;
h) Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

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

7.1.2.6. A AC SERPRO-JUS implementa as seguintes extensões, definidas como opcional pela ICP-Brasil.]

a) "*SubjectAlternativeName*", não critica, com o seguinte OtherName:
   - Certificados Cert-JUS **Equipamento Servidor** e Cert-JUS **Código Seguro**:
     - *Um campo* ***rfc822Name (OID= 2.5.29.17.1)*****, de preenchimento obrigatório**, contendo o e-mail institucional do responsável pelo certificado. Este campo deverá estar no formato IA5string;
     - O preenchimento do campo *rfc822Name*, contendo o e-mail institucional do responsável pelo certificado **é obrigatório.** Pode ser utilizado o e-mail da unidade organizacional responsável pelo certificado

b) "*Extended-key-usuage*", não critica, contendo os seguintes valores;
   - Certificados Cert-JUS **Código Seguro**:
     - "*code signing*" (OID 1.3.6.1.5.5.7.3.3);
   - Certificado Cert-JUS **Equipamento Servidor**:
     - "server authentication" (OID = 1.3.6.1.5.5.7.3.1);
     - "client authentication" (OID = 1.3.6.1.5.5.7.3.2).

7.1.3 IDENTIFICADORES DE ALGORITMO

7.1.3.1 Os algoritmos criptográficos utilizados para assinatura dos certificados pela ACSERPRO-JUS são os admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]:

7.1.3.1.1 Os certificados emitidos pela ACSERPRO-JUS v4 são assinados com o uso do algoritmo criptográfico SHA-256;

7.1.3.1.2 Os certificados emitidos pela ACSERPRO-JUS v3 e ACSERPRO-JUS v1 são assinados com o uso do algoritmo criptográfico SHA-1.

7.1.4 FORMATOS DE NOME

O DN (*Distinguished Name*) do certificado Cert-JUS **Equipamento Servidor** deve estar no formato:

C=**BR**,
O=**ICP-Brasil**,
OU=**Autoridade Certificadora da Justica – AC-JUS**
OU=**Cert-JUS Equipamento Servidor** – <*Tipo de Certificado*>
OU=<Órgão a que pertence><->><Sigla>
OU=<nome da Unidade Organizacional responsável pelo equipamento>

CN=<nome DNS (*Domain Name Service*) do equipamento ou nome da aplicação>

No formato acima, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores; os "<" e ">" não devem ser incluídos.

O CN (*Common Name*) deve conter a URL correspondente ao equipamento servidor, ou o nome da aplicação ou serviço, a que esse certificado se refere.

O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.
Todos os campos do DN são obrigatórios e devem ser preenchidos.

Para servidores do Poder Judiciário, a lista contendo os nomes dos órgãos e respectivas siglas padronizadas é disponibilizada no formulário de solicitação deste certificado na página da AC SERPRO-JUS.

Em caso de dúvida sobre a padronização de nomes e siglas de órgãos não constantes da lista citada no item anterior, a unidade administrativa da AC-JUS deve ser consultada.

Para servidores que não sejam do Poder Judiciário o nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente.

Exemplo :

URL do Equipamento: www.cjf.gov.br
Órgão onde está instalado: Conselho da Justiça Federal
Unidade organizacional responsável: Divisão de Operação e Serviços de Rede
DN:
C=BR,
O=ICP-Brasil,
OU= Autoridade Certificadora da Justica – AC-JUS,
OU=Cert-JUS Equipamento Servidor – A1
OU=Conselho da Justica Federal – CJF
OU=Divisao de Operacao e Servicos de Rede
CN=www.cjf.jus.br

O DN (*Distinguished Name*) do certificado Cert-JUS **Código Seguro** deve estar no formato:

C = BR,
O = ICP-Brasil,
OU = Autoridade Certificadora da Justica – AC-JUS
OU = Cert-JUS Codigo Seguro – <Tipo de Certificado>
OU = <nome da Unidade Organizacional responsável >
CN = <nome do órgão constante do CNPJ>

No formato acima, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores; os "<" e ">" não devem ser incluídos.

O CN (*Common Name*) deve conter a nome do órgão constante do CNPJ.

O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.

Para titulares do Poder Judiciário, a lista contendo os nomes dos órgãos e respectivas siglas padronizadas é disponibilizada no formulário de solicitação deste certificado na página da AC SERPRO-JUS.

Em caso de dúvida sobre a padronização de nomes e siglas de órgãos não constantes da lista citada no item acima, a unidade administrativa da AC-JUS deve ser consultada.

Exemplo :

Unidade Organizacional Responsável: DESIN – Secretaria de Desenvolvimento de Sistemas Internos
Nome do órgão constante do CNPJ: CONSELHO DA JUSTIÇA FEDRAL

DN:
C=BR, O=ICP-Brasil,
OU= Autoridade Certificadora da Justica – AC-JUS,
OU=Cert-JUS Codigo Seguro – A1
OU=DESIN - Secretaria de Desenvolvimento de Sistemas
CN=CONSELHO DA JUSTICA FEDERAL

7.1.5. Restrições de nome

7.1.5.1. Não se aplica.
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, poderão ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2^A

+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

Tabela 3 - Caracteres especiais admitidos em nomes

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

O OID atribuído a esta Política de Certificado é: 2.16.76.1.2.1.21

7.1.7 Uso da extensão *"Policy Constraints"*

Item não aplicável.

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 SERPRO-JUS.

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2. PERFIL DE LCR

7.2.1. Número de versão

As LCR geradas pela ACSERPRO-JUS segundo a 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 A ACSERPRO-JUS adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) **"*Authority Key Identifier*", não crítica**: contém o *hash* SHA-1 da chave pública da ACSERPRO-JUS;

b) **"*CRL Number*", não crítica:** contém número seqüencial para cada LCR emitida; e
c) **"*Authority Information Access*", não crítica:** contém somente o método de acesso id-ad-caIssuer, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação. Não deve ser utilizado nenhum outro método de acesso diferente de id-ad-caIssuer.

7.2.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

a) **"*Authority Key Identifier*", não critica;** contém o *hash SHA-1* da chave pública da AC que assina a LCR;
b) **"*CRL Number*", não crítica**: deve conter um número seqüencial para cada LCR emitida; e
c) **"*Authority Information Access*", não crítica:** deve conter somente o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. Não deve ser utilizado nenhum outro método de acesso diferente de id-ad-caIssuer.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes definem como é mantida e administrada a PC.

8.1. Procedimentos de mudança de especificação

As alterações nas especificações desta PC são realizadas pela AC SERPRO-JUS. Quaisquer modificações são submetidas à aprovação da ACSERPRO que as submeterá ao CG da ICP-Brasil.

8.2. Políticas de publicação e notificação

A cada nova versão, esta PC é publicada na página *Web* da AC SERPRO-JUS, cujo endereço vem a ser https://ccd.serpro.gov.br/acserprojus/ .

8.3 Procedimentos de aprovação

Esta PC foi submetida à aprovação da ACJUS, que por sua vez submeteu ao CG da ICP-Brasil, durante o processo de credenciamento da ACSERPRO-JUS conforme o estabelecido no documento "Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil". Como parte desse processo, além da conformidade com os documentos definidos pela ICP-Brasil, foi verificada a compatibilidade entre esta PC e a DPC da ACSERPRO-JUS.

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 sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[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 sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01