Declaração de Práticas de Certificação

Autoridade Certificadora

da Justiça

(DPC AC-JUS)

OID 2.16.76.1.1.19

Versão 5.1

1. INTRODUÇÃO

1.1. Visão Geral

Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da Justiça, AC-JUS, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, na execução dos seus serviços.

A AC-JUS possui certificados de primeiro nível na ICP-Brasil assinados pela AC Raiz da ICP-Brasil. Os certificados da AC-JUS contêm as chaves públicas correspondentes às chaves privadas utilizadas para assinar os certificados das AC de nível imediatamente subsequente ao seu e as suas LCR (Lista de Certificados Revogados).

A estrutura desta DPC AC-JUS está baseada no DOC ICP-5.0 versão 4.1, da ICP-Brasil e nas resoluções do Comitê Gestor da ICP-Brasil, CG ICP-Brasil.

1.2. Identificação

Este documento é chamado "Declaração de Práticas de Certificação da Autoridade Certificadora da Justiça" e comumente referido como "DPC AC-JUS". O Identificador de Objeto (OID) desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é 2.16.76.1.1.19.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

Esta DPC refere-se unicamente à Autoridade Certificadora da Justiça (AC-JUS) e encontra-se publicada no seu repositório, no seguinte endereço: http://www.acjus.jus.br/acjus/dpcacjus.pdf.

1.3.2. Autoridades de Registro

1.3.2.1. Os processos de identificação, cadastramento e recebimento de solicitações de renovação e revogação das AC de nível imediatamente subsequente ao da AC-JUS, são de competência de sua unidade administrativa, doravante chamada de AR-JUS. A AC-JUS disponibiliza e mantém atualizada na página http://www.acjus.jus.br as seguintes informações referentes à sua à AR-JUS:

a) o endereço de sua unidade administrativa – AR-JUS
b) meios para contato

1.3.3. Prestador de Serviços de Suporte

1.3.3.1. A AC-JUS disponibiliza e mantém atualizada o sítio web http://www.acjus.jus.br, contendo a relação de seus Prestadores de Serviço de Suporte – PSS vinculados.

1.3.3.2. PSS são entidades utilizadas pela AC e/ou suas AR para desempenhar atividades descritas em suas DPC e PC 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

1.3.4. Titulares de Certificado

A AC-JUS emite certificados para Autoridades Certificadoras de nível imediatamente subsequente ao seu. Os titulares dos certificados são órgãos do Poder Judiciário, Executivo, Legislativo, Ministério Público, Tribunais de Contas, entidades e pessoas jurídicas de direito público e privado, autorizados pela AC-JUS, e, cujos nomes aparecem no certificado digital, no campo "Distinguished Name (DN)".

1.3.5. Aplicabilidade

Os certificados definidos por esta DPC AC-JUS têm sua utilização exclusiva para a assinatura de certificados digitais das ACs de nível imediatamente subsequente ao seu e de sua Lista de Certificados Revogados (LCR).

1.4. Dados de Contato

Autoridade Certificadora da Justiça – AC-JUS

2.1.2. Obrigações da AR-JUS

As obrigações da AR-JUS são as abaixo relacionadas:

a) receber solicitações de cadastramento, de emissão e de revogação de certificados de AC de nível imediatamente subsequente ao seu;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) não se aplica;
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) disponibilizar os certificados emitidos pela AC-JUS aos seus respectivos solicitantes;
f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC-JUS e pela ICP-Brasil;
h) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP –Brasil;
i) não se aplica;
j) não se aplica;
k) garantir que todas as aprovações técnicas de solicitação de certificados sejam realizadas em instalações técnicas autorizadas, e
l) acompanhar, no ambiente off-line da AC candidata a subsequente, a geração do par de chaves e da solicitação do certificado;

2.1.3. Obrigações do Titular do Certificado

As obrigações das AC titulares de certificados emitido de acordo com esta DPC AC-JUS são as abaixo relacionadas:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
c) utilizar os seus certificados e suas respectivas chaves privadas de modo apropriado, conforme o previsto nesta DPC e em suas respectivas DPC e PC;
d) conhecer os seus direitos e obrigações, contemplados nesta DPC e em outros documentos aplicáveis da AC-JUS e da ICP-Brasil;
e) informar à AC-JUS qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
f) emitir certificados aos usuários finais, pessoa física ou jurídica, obedecendo os padrões e requisitos constantes do documento LEIAUTE DOS CERTIFICADOS DIGITAIS CERT-JUS[10];
g) operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementar, estabelecidas em conformidade com os documentos REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP BRASIL[2], REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP BRASIL[3], LEIAUTE DOS CERTIFICADOS CERT-JUS[10] e demais normas publicadas pela AC-JUS e pela ICP-Brasil.;
h) fornecer mensalmente relatórios de emissão de certificados, à AC-JUS.

2.1.4. Direitos da Terceira Parte (Relying Party)

2.1.4.1. Considera-se terceira parte, a parte usuária que confia no teor, validade e aplicabilidade do certificado digital.

2.1.4.2. Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos na PC correspondente.
b) verificar a qualquer tempo a validade do certificado, sendo este considerado válido quando:
c) não constar da LCR da AC emitente;
d) não estiver expirado; e
e) puder ser verificado com o uso de certificado válido da AC emitente.

2.4.3. Procedimentos de solução de disputa

2.4.3.1. Esta DPC prevalece sobre quaisquer outros documentos como planos, declarações, políticas, acordos e contratos que a AC-JUS venha a adotar. Podem haver documentos complementares ou normativos, os quais não podem contrariar esta DPC. Em caso de conflito o documento conflitante deve ser ignorado ou alterado.
2.4.3.2. Em caso de conflito entre esta DPC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nesse caso, esta DPC será alterada para a solução da disputa.
2.4.3.3. Os casos omissos deverão ser encaminhados para apreciação da AC Raiz.

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e renovação de certificados

O Comitê Gestor da AC-JUS poderá definir custos para emissão ou renovação de certificados de AC de nível imediatamente subsequente ao seu. A emissão e renovação de certificados de AC de nível imediatamente ao seu poderá estar condicionada à celebração de acordos ou convênios.

2.5.2. Tarifas de acesso ao certificado

Não há tarifas previstas pela AC-JUS para o acesso a seu certificado.

2.5.3. Tarifas de revogação ou de acesso à informação de status

Não há tarifas previstas pela AC-JUS para a revogação ou acesso a informações de status de certificados de AC de nível imediatamente subsequente ao seu.

2.5.4. Tarifas para outros serviços, tais como informação de política

Não há tarifas previstas pela AC-JUS outros serviços.

2.5.5. Política de reembolso

A AC-JUS não estabelece política de reembolso.

2.6. Publicação e Repositório

2.6.1. Publicação de informação da AC-JUS

A AC-JUS publica e disponibiliza informações, tais como certificados, LCR, sua DPC, entre outras, em página WEB, com disponibilidade de 99,50% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.
São publicados na página web da AC-JUS em http://www.acjus.jus.br:

a) os certificados da AC-JUS;
b) suas LCR;
c) esta DPC ;
d) não se aplica;
e) não se aplica;
f) não se aplica;
g) uma relação, regularmente atualizada dos PSS vinculados ;e
h) o documento LEIAUTE DOS CERTIFICADOS DIGITAIS CERT-JUS[10], contendo os perfis admitidos para os certificados emitidos na cadeia de certificação da AC-JUS e os requisitos para sua emissão.

2.6.2. Frequência de publicação

Os certificados e a LCR são publicados imediatamente após sua primeira emissão pela AC-JUS. As LCR são publicadas a cada 45 dias, no máximo, independentemente de haver alteração. Esta DPC AC-JUS, é publicada após aprovação pela AC Raiz da ICP-Brasil. As informações mencionadas neste item e no 2.6.1 serão publicadas sempre que sofrerem alterações.

2.8.2. Tipos de informações sigilosas

2.8.2.1. Todas as informações coletadas, geradas, transmitidas e mantidas pela AC-JUS e a AR-JUS são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3. Essas informações serão arquivadas de acordo com sua classificação, especificada na Política de Segurança.
2.8.2.2. Como princípio geral, nenhum documento, informação ou registro fornecido à AC-JUS ou AR-JUS deverá ser divulgado.

2.8.3. Tipos de informações não sigilosas

São consideradas informações não sigilosas:

a) os certificados e as LCR emitidos pela AC-JUS;
b) informações corporativas ou pessoais que necessariamente façam parte dos certificados ou de diretórios públicos;
c) não se aplica;
d) a DPC da AC-JUS;
e) versões públicas de Políticas de Segurança;
f) a conclusão dos relatórios de auditoria; e
g) o Leiaute de Certificados Digitais CERT-JUS.

2.8.4. Divulgação de informação de revogação/suspensão de certificado

2.8.4.1. A AC-JUS disponibiliza a lista de certificados revogados em seu repositório, http://www.acjus.jus.br. Os motivos que justificaram a revogação são mantidos confidenciais pela AC-JUS e pela AR-JUS, exceto quando:

a) o titular do certificado revogado autorizar expressamente a sua divulgação a terceiros;
b) esses motivos tenham sido publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da AC-JUS ou da AR-JUS;
c) tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC-JUS ou a AR-JUS, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

2.8.4.2. As razões para revogação do certificado sempre serão informadas para o seu titular.
2.8.4.3. A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

2.8.5. Quebra de sigilo por motivos legais

A AC-JUS tem o dever de fornecer documentos, informações ou registro sob sua guarda, mediante ordem judicial.

2.8.6. Informações a terceiros

Como diretriz geral nenhum documento, informação ou registro sob a guarda da AR-JUS ou AC-JUS, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

3.1.1.2. não se aplica;

3.1.1.3. não se aplica;

3.1.1.4. Será mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL [1].

3.1.1.4.1. não se aplica.

3.1.1.5. não se aplica

3.1.1.6. não se aplica.

3.1.1.7. não se aplica

3.1.1.8. não se aplica

3.1.2. Tipos de nomes

3.1.2.1. As AC de nível imediatamente subsequente ao da AC-JUS, titulares de certificados terão um nome que as identifique univocamente no âmbito da ICP-Brasil.

O DN (Distinguished Name) dos certificados deverá seguir o padrão definido no item 7.1.4.;
O atributo CN do DN deverá ser na forma:
"AC<espaço>subsequente<->JUS <indicador de versão>";
A formação do DN e demais definições encontram-se no documento LEIAUTE DOS CERTIFICADOS DIGITAIS CERT-JUS [10].

3.1.2.2. Certificados emitidos para AC subsequente não incluirão o nome da pessoa responsável.

3.1.3. Necessidade de nomes significativos

Para identificação dos titulares dos certificados emitidos, a AC-JUS faz uso de nomes significativos que possibilitam determinar a identidade da organização a que se referem.

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Os identificadores "Distinguished Name" (DN) são únicos para cada AC de nível imediatamente subsequente ao da AC-JUS. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509.
A extensão "Unique Identifiers" não será admitida para diferenciar as AC com nomes idênticos.

3.1.6. Procedimento para resolver disputa de nomes

A AC-JUS reserva-se o direito de tomar todas as decisões referentes a disputas de nomes das AC de nível imediatamente subsequente ao seu. Durante o processo de confirmação de identidade, a AC solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

3.1.10.1.3. A confirmação da identidade da organização e das pessoas físicas, será feita nos seguintes termos:

a) apresentação do rol de documentos elencado no item 3.1.10.2;
b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo certificado; e
c) presença física dos representantes legais e do responsável pelo uso do certificado e assinatura do termo de titularidade de que trata o item 4.1.1.

3.1.10.2. Documentos para efeitos de identificação de uma organização

3.1.10.2.1. A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos a sua habilitação jurídica:
    i. se pessoa jurídica cuja criação se deu ou foi autorizada por lei, cópia do ato constitutivo e CNPJ;
    ii. se entidade privada:
        1. ato constitutivo, devidamente registrado no órgão competente; e
        2. documentos da eleição de seus administradores, quando aplicável;
b) Relativos a sua habilitação fiscal:
    i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
    ii. prova de inscrição no Cadastro Específico do INSS – CEI.

3.1.10.3. Informações contidas no certificado para uma organização

3.1.10.3.1. não se aplica.

3.1.10.3.2. não se aplica

3.1.11. Autenticação da identidade de equipamento ou aplicação

Não se aplica.

3.1.12. Autenticação de identificação de equipamento para certificado CF-e-SAT

Não se aplica.

4.2. Emissão de Certificado

4.2.1. A emissão de um certificado pela AC-JUS é feita em cerimônia específica, com a presença de representantes da AC-JUS, da AC habilitada, convidados e testemunhas do PSS, na qual são registrados todos os procedimentos executados.

A AC-JUS garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 10 (dez) dias úteis após o recebimento da solicitação citada no item 4.1.3.
A emissão dos certificados das AC de nível imediatamente subsequente à AC-JUS é feita em equipamentos que operam off-line. A AC-JUS entrega o certificado emitido, no padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], para os representantes legais da AC habilitada.

4.2.2. O certificado é considerado válido a partir do momento de sua emissão.

4.3. Aceitação de Certificado

4.3.1. A AC-JUS garante que as informações contidas no certificado emitido para uma AC de nível imediatamente subsequente ao seu foram verificadas de acordo com esta DPC.

4.3.2. A AC atestará através de seus representantes legais, mediante assinatura do "Termo de Acordo", o recebimento do certificado emitido.

4.3.3. A aceitação do certificado se dá após a verificação pela AC ou na primeira utilização da chave privada correspondente

b) As solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;
c) As justificativas para a revogação de um certificado serão documentadas; e
d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado, e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado na base de dados da AC.

4.4.3.3. Não se aplica.
4.4.3.4. O prazo máximo para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação é de 12 (doze) horas.
4.4.3.5. A AC responsável responderá plenamente por todos os danos causados pelo uso do certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.
4.4.3.6. Não se aplica.

4.4.4. Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1.
4.4.4.2. não se aplica

4.4.5. Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.6. Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS

4.4.7. Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.8. Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.9. Frequência de emissão de LCR

4.4.9.1. A frequência definida para a emissão de LCR referente a certificados de AC de nível imediatamente subsequente ao da AC-JUS é de 45 dias, no máximo.
4.4.9.2. Não se aplica.
4.4.9.3. A frequência máxima para emissão de LCR é de 45 dias. Em caso de revogação de certificado emitido pela AC-JUS, será emitida nova LCR no prazo previsto no item 4.4.3 e notificadas todas as AC de nível imediatamente subsequente ao seu e a AC-Raiz.
4.4.9.4. Não se aplica.

4.4.10. Requisitos para verificação de LCR

4.4.10.1. Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.
4.4.10.2. A autenticidade da LCR deverá também ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

4.4.11. Disponibilidade para revogação/verificação de status on-line

A AC-JUS não disponibiliza recursos para revogação on-line de certificados.

4.4.12. Requisitos para verificação de revogação on-line

Não se aplica.

4.5.1.7. Não se aplica.

4.5.2. Frequência de auditoria de registros (logs)

4.5.2.1. A análise dos registros de auditoria será realizada mensalmente, sempre que houver utilização de seu sistema de certificação (o equipamento é off-line permanecendo desligado a maior parte do tempo) ou em caso de suspeita de comprometimento da segurança.
4.5.2.2. Os registros de auditoria são analisados pelo pessoal operacional da AC-JUS. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando-se que não foram alterados, em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3. Período de Retenção para registros (logs) de Auditoria

A AC-JUS mantém localmente, nas instalações do seu PSS, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4. Proteção de registro (log) de Auditoria

4.5.4.1. Os equipamentos da AC-JUS, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança.
4.5.4.2. A inspeção contínua dos diversos registros dos sistemas é feita por meio das ferramentas nativas do sistema operacional, do banco de dados e do aplicativo de AC, e estão disponíveis somente para leitura. Pode ser feita também por relatórios emitidos a partir destas ferramentas. Estes dados de auditoria são coletados e armazenados toda a vez que existir utilização do equipamento em uma sala de arquivos de nível 3 de segurança.
4.5.4.3. Os registros de auditoria gerados eletrônica ou manualmente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da Política de Segurança da ICP-Brasil.

4.5.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria

A AC-JUS executa procedimentos de backup de todo o sistema de certificação, sempre que houver utilização do mesmo, seguindo scripts previamente desenvolvidos para estas atividades.

4.5.6. Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da AC-JUS é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC-JUS, pelo sistema de controle de acesso e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de log-in e log-out	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional

4.6.2. Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:

a) as LCR e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
b) as cópias dos documentos de identificação apresentados no momento da solicitação e da revogação de certificados e os termos de titularidade e responsabilidade serão retidos, no mínimo 10 (dez) anos a contar da data de expiração ou revogação do certificado. Prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado; e
c) as demais informações, inclusive registros de auditoria são retidas por, no mínimo, 7 (sete) anos.

4.6.3. Proteção de arquivos

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da ICP-Brasil. Mídias de arquivos são guardadas em local seguro, sendo que a proteção criptográfica das mídias é adotada quando a classificação da informação assim o exigir. Também são protegidas de fatores ambientais como temperatura, umidade e magnetismo.

4.6.4. Procedimentos para cópia de segurança (backup) de arquivos

4.6.4.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC-JUS, protegido com o mesmo tipo de proteção utilizada no arquivo principal.
4.6.4.2. As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.
4.6.4.3. A AC-JUS garante que a verificação da integridade dessas cópias de segurança, é realizada no mínimo, a cada 6 (seis) meses.

4.6.5. Requisitos para datação (time-stamping) de registros

Os servidores da AC-JUS são sincronizados com a hora GMT fornecida pelo Observatório Nacional. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.
No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.6. Sistema de coleta de dados de arquivo

O sistema de coleta de dados de arquivos da AC-JUS é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
Solicitações de certificados	Automático e manual	Software de AC/AR e pessoal de operações
Solicitações de revogação de certificados Notificações de comprometimento de chaves privadas	Automático e manual Manual	Software de AC/AR e pessoal de operações Pessoal de operações
Emissões e revogações de certificados Emissões de LCR	Automático Automático	Software de AC/AR Software de AC/AR
Correspondências formais	Manual	Pessoal de operações

4.6.7. Procedimentos para obter e verificar informação de arquivo

4.8.4. Segurança dos recursos após desastre natural ou de outra natureza

A AC-JUS possui um PCN que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC-JUS quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.
O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC-JUS faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a AC-JUS para tornar acessível os registros lógicos mantidos dentro do software. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

4.8.5. Atividades das Autoridades de Registro

A AR-JUS por ser interna à AC-JUS utiliza o PCN da própria AC-JUS onde são descritos os procedimentos previstos para recuperação total ou parcial das atividades da AC-JUS, entre os quais:

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios;
b) identificação e concordância de todas as responsabilidades e procedimentos definidos;
c) implementação dos procedimentos de emergência que permitam recuperação e restauração nos prazos necessários;
d) documentação dos processos e procedimentos acordados;
e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
f) teste e atualização dos planos.

4.9. Extinção dos serviços de AC-JUS, AR-JUS ou PSS

4.9.1. A AC-JUS observa os procedimentos descritos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.9.2. Quando for necessário encerrar as atividades da AC-JUS, AR-JUS ou do PSS, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes, inclusive:

a) notificar a AC Raiz da ICP-Brasil;
b) notificar todas as entidades subordinadas;
c) providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;
d) a transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-JUS, AR-JUS ou PSS;
e) preservar qualquer registro não transferido a um sucessor;
f) a AC-JUS, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e
g) caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

5. Controles de Segurança Física, Procedimental e de Pessoas

5.1. Controle Físico

5.1.1. Construção e localização das instalações de AC

5.1.1.1. A operação da AC-JUS é executada dentro de um ambiente físico seguro em área de instalação altamente protegida. A localização e o sistema de certificação utilizado para a operação da AC-JUS não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos. Nenhuma das linhas telefônicas dentro do ambiente de certificação da AC oferece suporte a modem.
5.1.1.2. Todas as instalações da AC- JUS, relevantes para os controles de segurança física, foram por técnicos especializados, especialmente os descritos a seguir:

5.1.2.1.9. No quarto nível, todas as paredes o piso e o teto são revestidos de aço e concreto. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem a chamada sala cofre - possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. A sala cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.

5.1.2.1.11. São três os ambientes de quarto nível abrigados pela sala cofre:

a) Sala de equipamentos de produção on-line e cofre de armazenamento.
b) Sala de equipamentos de produção off-line e cofre de armazenamento.
c) Equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores)

5.1.2.1.12. O quinto nível – ou nível 5– é interno aos ambientes de nível 4, e compreende cofres e gabinetes trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em nível 5 ou superior.

5.1.2.1.13. Para garantir a segurança do material armazenado o cofre ou o gabinete obedecem às seguintes especificações mínimas:

a) Ser feito em aço ou material de resistência equivalente;
b) Possuir tranca com chave.

5.1.2.1.14. O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível, ou hardware criptográfico. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da C-JUS estão armazenados em um desses depósitos

5.1.2.2. Sistema físico de detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmaras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2. As mídias de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes.

5.1.2.2.4. Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar de ser satisfeito, ocorre a reativação automática dos sensores de presença.

5.1.4. Exposição à água nas instalações de AC

A estrutura inteiriça do ambiente de nível 4, construído na forma de célula estanque, provê proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5. Prevenção e proteção contra incêndio nas instalações de AC

5.1.5.1. Todas as instalações da AC-JUS possuem sistemas de prevenção contra incêndio. Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.
5.1.5.2. Nas instalações da AC-JUS não é permitido fumar ou portar objetos que produzam fogo ou faísca.
5.1.5.3. A sala cofre possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala cofre são eclusas, uma porta só se abre quando a anterior está fechada.
5.1.5.4. Em caso de incêndio nas instalações da AC-JUS, a temperatura interna da sala cofre não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.6. Armazenamento de mídia nas instalações de AC

A AC-JUS atende a norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7. Destruição de lixo nas instalações de AC

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo;
5.1.7.2. Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos;

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

As instalações de backup atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não serão atingidas e tornar-se-ão totalmente operacionais em, no máximo, 48 (quarenta e oito) horas.

5.1.9. Instalações Técnicas de AR

Não se aplica.

5.2. Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC-JUS, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.
5.2.1.2. A AC-JUS estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as ações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.
5.2.1.3. Todos os operadores do sistema de certificação da AC-JUS recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.
5.2.1.4. Quando um empregado se desliga da AC, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC-JUS e da AR vinculada, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e mecanismos de segurança da AC-JUS e das AR vinculadas;
b) Sistema de certificação em uso na AC-JUS;
c) Procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9, 3.1.10 e 3.1.11; e
e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC-JUS e da AR vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC-JUS. Treinamentos de reciclagem são realizados pela AC-JUS sempre que necessário.

5.3.5. Frequência e sequência de rodízios de cargos

A AC-JUS não implementa rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC-JUS suspenderá o seu acesso ao sistema de certificação e tomará as medidas administrativas e legais cabíveis.
5.3.6.2. O processo administrativo referido acima conterá, no mínimo, os seguintes itens:

a) relato da ocorrência com "modus operandi";
b) identificação dos envolvidos;
c) eventuais prejuízos causados;
d) punições aplicadas, se for o caso; e
e) conclusões.

5.3.6.3. Concluído o processo administrativo, a AC-JUS encaminhará suas conclusões à AC Raiz.
5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

a) advertência;
b) suspensão por prazo determinado; ou
c) impedimento definitivo de exercer funções no âmbito da AC-JUS e da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC-JUS, da AR Vinculada, do PSS e das AC de nível imediatamente subsequente, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, será contratado conforme o estabelecido nas Política de Segurança da ICP Brasil[8] e na Política de Segurança da AC-JUS.

5.3.8. Documentação disponibilizada ao pessoal

5.3.8.1. A AC-JUS disponibiliza para todo o seu pessoal, para as AC de nível imediatamente subsequente ao seu e para a AR vinculada :

a) esta DPC;
b) não se aplica;
c) a Política de Segurança da ICP-Brasil[8];
d) documentação operacional relativa às suas atividades; e
e) contratos, normas e políticas relevantes para suas atividades.

6.1.8. Geração de chave por hardware ou software

6.1.8.1. O processo de geração do par de chaves da AC-JUS é feito por hardware criptográfico com padrão de segurança "Homologação da ICP-Brasil NSH-3", definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].
6.1.8.2. Não se aplica.

6.1.9. Propósitos de uso de chave (conforme campo "Key usage" na X.509 v3)

6.1.9.1. As chaves criptográficas dos titulares (AC subsequente) de certificados emitidos pela AC-JUS poderão ser utilizadas apenas para assinatura dos certificados por elas emitidos e de suas LCR.
6.1.9.2. A chave privada da AC-JUS é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2. Proteção da Chave Privada

As chaves privadas da AC-JUS são geradas, armazenadas e utilizadas apenas em hardware criptográfico com padrão de segurança "Homologação da ICP-Brasil NSH-3", definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], não havendo, portanto, tráfego das mesmas em nenhum momento.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. Toda a geração e armazenamento da chave da AC-JUS, e também operações de assinatura de certificados pela AC-JUS, são realizadas em um módulo de hardware criptográfico com padrão de segurança "Homologação da ICP-Brasil NSH-3" de acordo com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].
6.2.1.2. Os módulos criptográficos das AC subsequentes à AC-JUS devem adotar padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.2. Controle "n de m' para chave privada

6.2.2.1. A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC-JUS é dividida em "9" partes e distribuídas por "9" custodiantes designados pela AC-JUS (m).
6.2.2.2. É necessária a presença de no mínimo "2" custodiantes (n) para a ativação do componente e a consequente utilização da chave privada.

6.2.3. Recuperação (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas, das AC de nível imediatamente subsequente. Isto é, não se permite que terceiros possam legalmente obter uma chave privada com o consentimento de seu titular.

6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. Como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.
6.2.4.2. A AC-JUS mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.
6.2.4.3. A AC-JUS não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subsequentes ao seu.
6.2.4.4. A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+, ou outros definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas dos titulares de certificados emitidos pela AC-JUS não são arquivadas.

6.4.2. Proteção dos dados de ativação.

6.4.2.1. Os dados de ativação das chaves privadas da AC-JUS são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.
6.4.2.2. Não se aplica.

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

6.5.1.1. A AC-JUS garante que a geração de seu par de chaves é realizada em ambiente off-line, para impedir o acesso remoto não autorizado.
6.5.1.2. Os requisitos gerais de segurança computacional dos equipamentos utilizados para a geração dos pares de chaves criptográficas das AC titulares de certificados emitidos pela AC-JUS, devem ser os mesmos descritos no item abaixo para os computadores servidores da AC-JUS.
6.5.1.3. Os computadores servidores, utilizados pela AC-JUS, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) Controle de acesso aos serviços e perfis da AC-JUS;
b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC-JUS;
c) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
d) Geração e armazenamento de registros de auditoria da AC-JUS;
e) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) Mecanismos para cópias de segurança (backup).

6.5.1.4. Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física
6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC-JUS ou da AC subordinada, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC-JUS ou AC subsequente.Todos esses eventos são registrados para fins de auditoria.
6.5.1.6. Qualquer equipamento incorporado à AC-JUS ou às AC subsequente é preparado e configurado como previsto na política de segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A AC-JUS aplica configurações de segurança definida como EAL3, baseada na Common Criteria e desenvolvida para o sistema operacional SUSE LINUX pela SUSE, que disponibiliza as atualizações deste sistema operacional utilizado nos servidores do Sistema de Certificação Digital do PSS da AC-JUS.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.
6.5.3.2. Não se aplica.

6.7.1.4. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (patches), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.
6.7.1.5. O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2. Firewall

6.7.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Um firewall promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – chamada "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC
6.7.2.2. O software de firewall, entre outras características, implementa registros de auditoria.

6.7.3. Sistema de detecção de intrusão

6.7.3.1. O sistema de detecção de intrusão pode ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao firewall ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do firewall.
6.7.3.2. O sistema de detecção de intrusão tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.
6.7.3.3. O sistema de detecção de intrusão provê o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4. Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro é, no mínimo, diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela AC-JUS para o armazenamento de sua chave privada está em conformidade com o padrão "Homologação da ICP-Brasil NSH-3" definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].
O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
b) a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.
d) Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

7. Perfis de Certificado e LCR

7.1. Diretrizes Gerais

7.1.1. Nos itens seguintes são descritos os aspectos dos certificados e LCR emitidos pela AC-JUS.

7.2.4. Formatos de nome

Para os certificados emitidos sob esta DPC AC-JUS, o nome da AC 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= Autoridade Certificadora da Justiça – AC-JUS

OU = <SMIME, SSL ou Codesigning, de acordo com o tipo de uso escolhido conforme a IN 12/2016 do ITI>

CN= nome da AC titular

O CN deverá estar na forma "AC <nome da AC titular>-JUS <sigla do tipo de uso> <identificador de versão>"

7.2.5. Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC-JUS são as seguintes:

a) não serão utilizados sinais de acentuação, tremas ou cedilhas;
b) aplicam-se as restrições gerais estabelecidas no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

7.2.6. OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC-JUS após conclusão do processo de seu credenciamento, é 2.16.76.1.1.19.

7.2.7. Uso da extensão "Policy Constraints"

A extensão "Policy Constraints" poderá ser utilizada, da forma definida na RFC 5280, em certificados emitidos pela AC-JUS.

7.2.8. Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web (URL) da DPC da AC-JUS.

7.2.9. Semântica de processamento para extensões criticas

Extensões críticas são interpretadas, no âmbito da AC-JUS, conforme a RFC 5280.

7.3. Perfil de LCR

7.3.1. Número (s) de versão

As LCR geradas pela AC-JUS implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2. Extensões de LCR e de suas entradas

7.3.2.1. A AC-JUS adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC-JUS que assina a LCR.
b) "CRL Number", não crítica: contém número seqüencial para cada LCR emitida pela AC-JUS.

8. Administração de Especificação

8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta DPC da AC-JUS será submetida previamente à aprovação da AC RAIZ.

9.3. Os documentos a seguir são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br.

Ref	Nome do documento	Código
[4]	TERMOS DE TITULARIDADE	ADE-ICP-05.B

9.4. O documento a seguir é aprovado pelo Comitê Gestor da AC-JUS, podendo ser alterado quando necessário,, mediante publicação no sítio da AC-JUS.

9.4.1. O sítio da AC-JUS em http://www.acjus.jus.br, publica a versão mais atualizada desse documento.

Ref	Nome do documento	
[10]	LEIAUTE DOS CERTIFICADOS CERT-JUS	AC-JUS - 02