



Declaração de Práticas de Certificação
da
Autoridade Certificadora
da Justiça

(DPC AC-JUS)

OID 2.16.76.1.1.1.9

Versão 2.0



Sumário

1.INTRODUÇÃO	7
1.1.Visão Geral	7
1.2.Identificação	7
1.3.Comunidade e Aplicabilidade	7
1.3.1. Autoridades Certificadoras	7
1.3.2. Autoridades de Registro	7
1.3.3.Prestador de Serviços de Suporte	7
1.3.4.Titulares de Certificado	8
1.3.5. Aplicabilidade	8
1.4.Dados de Contato	8
1.4.1. Pessoas de Contato	8
2.DISPOSIÇÕES GERAIS	8
2.1.Obrigações e Direitos	8
2.1.1.Obrigações da AC-JUS	8
2.1.2. Obrigações da AR-JUS	9
2.1.3.Obrigações do Titular do Certificado	10
2.1.4.Direitos da Terceira Parte (Relying Party)	10
2.1.5. Obrigações do Repositório	10
2.2.Responsabilidades	10
2.2.1.Responsabilidades da AC-JUS	10
2.2.2.Responsabilidades da AR	10
2.3.Responsabilidade Financeira	11
2.3.1. Indenizações devidas pela terceira parte usuária (Relying Party)	11
2.3.2.Relações Fiduciárias	11
2.3.3. Processos Administrativos	11
2.4.Interpretação e Execução	11
2.4.1.Legislação	11
2.4.2.Forma de interpretação e notificação	11
2.4.3.Procedimentos de solução de disputa	11
2.5.Tarifas de Serviço	11
2.5.1.Tarifas de emissão e renovação de certificados	11
2.5.2. Tarifas de acesso ao certificado	12
2.5.3. Tarifas de revogação ou de acesso à informação de status	12
2.5.4. Tarifas para outros serviços, tais como informação de política	12
2.5.5. Política de reembolso	12
2.6.Publicação e Repositório	12
2.6.1. Publicação de informação da AC-JUS	12
2.6.2. Frequência de publicação	12
2.6.3.Controles de acesso	13
2.6.4. Repositórios	13
2.7.Fiscalização e Auditoria de conformidade	13
2.8.Sigilo	13
2.8.1.Disposições Gerais	13
2.8.2.Tipos de informações sigilosas	14
2.8.3. Tipos de informações não sigilosas	14



2.8.4.Divulgação de informação de revogação/suspensão de certificado	14
2.8.5. Quebra de sigilo por motivos legais	14
2.8.6.Informações a terceiros	14
2.8.7. Divulgação por solicitação do titular.....	14
2.8.8. 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	16
3.1.3.Necessidade de nomes significativos.....	16
3.1.4. Regras para interpretação de vários tipos de nomes	16
3.1.5. Unicidade de nomes.....	16
3.1.6. Procedimento para resolver disputa de nomes.....	16
3.1.7.Reconhecimento, autenticação e papel de marcas registradas	16
3.1.8. Método para comprovar a posse de chave privada.....	16
3.1.9. Autenticação da Identidade de um Indivíduo.....	17
3.1.10. Autenticação da Identidade de uma organização	18
3.1.11. Autenticação da identidade de equipamento ou aplicação	18
3.2.Geração de novo par de chaves antes da expiração do atual	18
3.3.Criação de novo par de chaves após expiração ou revogação	18
3.4.Solicitação de Revogação.....	19
4. REQUISITOS OPERACIONAIS	19
4.1.Solicitação de Certificado	19
4.2.Emissão de Certificado.....	19
4.3.Aceitação de Certificado	19
4.4.Suspensão e Revogação de Certificado	20
4.4.1. Circunstâncias para revogação	20
4.4.2.Quem pode solicitar revogação.....	20
4.4.3.Procedimento para solicitação de revogação.....	20
4.4.4.Prazo para solicitação de revogação.....	21
4.4.5. Circunstâncias para suspensão	21
4.4.6. Quem pode solicitar suspensão	21
4.4.7. Procedimento para solicitação de suspensão	21
4.4.8. Limites no período de suspensão.....	21
4.4.9.Freqüência de emissão de LCR	21
4.4.10.Requisitos para verificação de LCR.....	22
4.4.11. Disponibilidade para revogação/verificação de status on-line	22
4.4.12. Requisitos para verificação de revogação on-line	22
4.4.13.Outras formas disponíveis para divulgação de revogação.....	22
4.4.14. Requisitos para verificação de outras formas de divulgação de revogação	22
4.4.15.Requisitos especiais para o caso de comprometimento de chave	22
4.5.Procedimentos de Auditoria de Segurança	22
4.5.1. Tipos de Evento Registrados	22
4.5.2.Freqüência de auditoria de registros (logs)	23
4.5.3.Período de Retenção para registros (logs) de Auditoria.....	23
4.5.4. Proteção de registro (log) de Auditoria	23
4.5.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria	24



4.5.6. Sistema de coleta de dados de auditoria	24
4.5.7. Notificação de agentes causadores de eventos	24
4.5.8. Avaliações de vulnerabilidade	24
4.6. Arquivamento de Registros	25
4.6.1. Tipos de registros arquivados	25
4.6.2. Período de retenção para arquivo	25
4.6.3. Proteção de arquivos	25
4.6.4. Procedimentos para cópia de segurança (backup) de arquivos	25
4.6.5. Requisitos para datação (time-stamping) de registros	25
4.6.6. Sistema de coleta de dados de arquivo	25
4.6.7. Procedimentos para obter e verificar informação de arquivo	26
4.7. Troca de chave	26
4.8. Comprometimento e Recuperação de Desastre	26
4.8.1. Recursos computacionais, software ou dados corrompidos	26
4.8.2. Certificado de entidade revogado	26
4.8.3. Chave de entidade comprometida	27
4.8.4. Segurança dos recursos após desastre natural ou de outra natureza	27
4.8.5. Atividades das Autoridades de Registro	27
4.9. Extinção dos serviços de AC-JUS, AR-JUS ou PSS	27
5. Controles de Segurança Física, Procedimental e de Pessoas	28
5.1. Controle Físico	28
5.1.1. Construção e localização das instalações	28
5.1.2. Acesso físico	28
5.1.3. Níveis de Acesso	28
5.1.4. Sistema de Controle de Acesso	30
5.1.5. Mecanismos de emergência	30
5.1.6. Energia e ar condicionado	30
5.1.7. Exposição à água	31
5.1.8. Prevenção e proteção contra incêndio	31
5.1.9. Armazenamento de mídia	31
5.1.10. Destruição de lixo	31
5.1.11. Instalações de segurança (backup) externas (off-site)	31
5.1.12. Instalações Técnicas de AR	32
5.2. Controles Procedimentais	32
5.2.1. Perfis qualificados	32
5.2.2. Número de pessoas necessário por tarefa	32
5.2.3. Identificação e autenticação para cada perfil	32
5.3. Controles de Pessoal	32
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade	33
5.3.2. Procedimentos de Verificação de Antecedentes	33
5.3.3. Requisitos de treinamento	33
5.3.4. Frequência e requisitos para reciclagem técnica	33
5.3.5. Frequência e seqüência de rodízios de cargos	33
5.3.6. Sanções para ações não autorizadas	34
5.3.7. Requisitos para contratação de pessoal	34
5.3.8. Documentação disponibilizada ao pessoal	34
6. Controles Técnicos de Segurança	34
6.1. Geração e Instalação do Par de chaves	34



6.1.1.Geração do Par de Chaves.....	34
6.1.2.Entrega da chave privada à entidade titular.....	35
6.1.3.Entrega da chave pública para emissor de certificado.....	35
6.1.4.Disponibilização de chave pública da AC-JUS para usuários.....	35
6.1.5.Tamanhos de chave.....	35
6.1.6.Geração de parâmetros de chaves assimétricas.....	35
6.1.7.Verificação da qualidade dos parâmetros.....	35
6.1.8.Geração de chave por hardware ou software.....	36
6.1.9.Propósitos de uso de chave (conforme campo “Key usage” na X.509 v3).....	36
6.1.10.Proteção da Chave Privada.....	36
6.1.11. Padrões para módulo criptográfico.....	36
6.1.12.Controle “n de m’ para chave privada.....	36
6.1.13.Recuperação (escrow) de chave privada.....	36
6.1.14. Cópia de segurança (backup) de chave privada.....	36
6.1.15. Arquivamento de chave privada.....	37
6.1.16.Inserção de chave privada em módulo criptográfico.....	37
6.1.17.Método de ativação de chave privada.....	37
6.1.18.Método de desativação de chave privada.....	37
6.1.19. Método de destruição de chave privada.....	37
6.2.Outros Aspectos do Gerenciamento do Par de Chaves.....	37
6.2.1. Arquivamento de chave pública.....	37
6.2.2.Períodos de uso para as chaves pública e privada.....	38
6.3.Dados de ativação.....	38
6.3.1. Geração e instalação dos dados de ativação.....	38
6.3.2. Proteção dos dados de ativação.....	38
6.3.3. Outros aspectos dos dados de ativação.....	38
6.4.Controles de Segurança dos computadores.....	38
6.4.1. Requisitos técnicos específicos de segurança computacional.....	38
6.4.2.Classificação da segurança computacional.....	39
6.4.3. Controle de segurança para as Autoridades de Registro.....	39
6.5.Controles Técnicos do Ciclo de Vida.....	39
6.5.1. Controles de desenvolvimento de sistemas.....	39
6.5.2. Controle de gerenciamento de segurança.....	39
6.5.3.Classificação de segurança de ciclo de vida.....	40
6.6.Controles de Segurança de Rede.....	40
6.6.1. Diretrizes Gerais.....	40
6.6.2.Firewall.....	40
6.6.3.Sistema de detecção de intrusão (IDS).....	40
6.6.4.Registro de acessos não autorizados à rede.....	41
6.7.Controles de Engenharia do Módulo Criptográfico.....	41
7.Perfis de Certificado e LCR.....	41
7.1.Diretrizes Gerais.....	41
7.2.Perfil do Certificado.....	41
7.2.1. Número(s) de versão.....	41
7.2.2. Extensões de certificados.....	41
7.2.3. Identificadores de algoritmos.....	42
7.2.4. Formatos de nome.....	42
7.2.5.Restrições de nome.....	42



Autoridade Certificadora da Justiça
Declaração de Práticas de Certificação
DPC AC-JUS

7.2.6.OID (Object Identifier) de DPC.....	43
7.2.7. Uso da extensão “Policy Constraints”.....	43
7.2.8.Sintaxe e semântica dos qualificadores de política	43
7.2.9.Semântica de processamento para extensões críticas.....	43
7.3.Perfil de LCR.....	43
7.3.1. Número (s) de versão	43
7.3.2.Extensões de LCR e de suas entradas.....	43
8.Administração de Especificação.....	43
8.1.Procedimentos de mudança de especificação	43
8.2.Políticas de publicação e de notificação	43
8.3.Procedimentos de aprovação.....	44
9.Documentos referenciados	44



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*



Autoridade Certificadora da Justiça
Declaração de Práticas de Certificação
DPC AC-JUS

UF - Unidade de Federação

URL - Uniform Resource Location



1. INTRODUÇÃO

1.1. Visão Geral

- 1.1.1. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da Justiça, AC-JUS, integrante da Infra-estrutura de Chaves Públicas Brasileira, ICP-Brasil, na execução dos seus serviços.
- 1.1.2. A AC-JUS possui um certificado de primeiro nível na ICP-Brasil assinado pela AC Raiz da ICP-Brasil. O certificado da AC-JUS contém a chave pública correspondente à chave privada utilizada para assinar os certificados das AC de nível imediatamente subsequente ao seu e a sua LCR (Lista de Certificados Revogados).
- 1.1.3. A AC-JUS utilizará o ambiente e os serviços do Serviço Federal de Processamento de Dados - SERPRO para hospedar, operar e dar manutenção às suas atividades.
- 1.1.4. A estrutura desta DPC AC-JUS está baseada nas resoluções do Comitê Gestor da ICP-Brasil, CG ICP-Brasil, e na RFC 2527 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Framework.

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 **2.16.76.1.1.1.9**.

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 na página: <http://www.acjus.gov.br/acjus/dpcacjus.pdf>.

1.3.2. Autoridades de Registro

Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência da AC-JUS através de sua Autoridade de Registro - AR, doravante chamada de AR-JUS.

A AC-JUS disponibiliza e mantém atualizadas na página <http://www.acjus.gov.br> as seguintes informações referentes às Autoridades de Registros – AR, credenciadas:

- 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 o caso.

1.3.3. Prestador de Serviços de Suporte



A AC-JUS disponibiliza e mantém atualizada a página web <http://www.acjus.gov.br> contendo a relação de todos os seus Prestadores de Serviço de Suporte – PSS vinculados, seja diretamente seja por intermédio de suas AR.

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, entidades e pessoas jurídicas de direito público e privado, autorizadas pela AR-JUS a receberem certificados digitais emitidos 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 e de Lista de Certificados Revogados (LCR).

1.4. Dados de Contato

Conselho da Justiça Federal
Autoridade Certificadora da Justiça – AC-JUS
Endereço: SAFS - Quadra 06 - Lote 01 - Trecho III
Bloco F - 3o andar – CJF/STI/ACJUS
CEP 70095-900, Brasília – DF
Telefone: (61) 3319-9841
Página Web: <http://www.acjus.gov.br>
E-mail: acjus@cjf.gov.br

1.4.1. Pessoas de Contato

Nome: Paulo Martins Inocência
E-mail: paulo.martins@acjus.gov.br

Nome: Wilson Nogueira de Aquino Jr.
E-mail: wilson.aquino@acjus.gov.br

Nome: Edicarlos Caixeta Borges
E-mail: edicarlos@acjus.gov.br

Endereço: SAFS - Quadra 06 - Lote 01 - Trecho III
Bloco F - 3o andar - CJF/STI/ACJUS
CEP 70095-900, Brasília – DF
Telefones: (61) 3319-9841 – 3319-9752 – 3319-9753

2. DISPOSIÇÕES GERAIS

2.1. Obrigações e Direitos

2.1.1. Obrigações da AC-JUS



As obrigações da AC-JUS são as abaixo relacionadas:

- a) Operar de acordo com esta DPC e com a PC implementada;
- b) Gerar e gerenciar os seus pares de chaves criptográficas;
- c) Assegurar a proteção de suas chaves privadas;
- d) Notificar a AC Raiz da ICP-Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
- e) Notificar as AC de nível imediatamente subsequente ao seu quando ocorrer suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- f) Distribuir o seu próprio certificado;
- g) Emitir, expedir e distribuir os certificados das AC de nível imediatamente subsequente ao seu;
- h) Informar a emissão do certificado ao respectivo solicitante;
- i) Revogar os certificados por ela emitidos;
- j) Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);
- k) Publicar em sua página web <http://www.acjus.gov.br> a DPC AC-JUS e a PC AC-JUS aprovadas e implementadas;
- l) publicar em sua página web as informações definidas no item 2.6.1.2 deste documento;
- m) publicar em sua página web informações sobre o descredenciamento de AR bem como sobre extinção de instalação;
- n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web ;
- o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil;
- p) adotar as medidas de segurança e controle previstas na DPC, PC e política de segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios e procedimentos da ICP-Brasil;
- q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- s) manter e testar regularmente seu Plano de Continuidade do Negócio;
- t) exigir manutenção de seguro de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, pelas AC de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil. À AC-JUS, por ser órgão da administração direta não cabe a contratação de seguro de responsabilidade civil;
- u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas condicionantes e limitações determinadas pela legislação vigente;
- v) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos;
- w) não emitir certificados com prazo de validade que se estenda além do prazo de validade de seu próprio certificado; e
- x) fiscalizar suas AC subsequentes além das respectivas AR e PSS, habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor (CG) da ICP-Brasil.

2.1.2. Obrigações da AR-JUS

As obrigações da AR-JUS são as abaixo relacionadas:

- a) receber solicitações de emissão e revogação de certificados;



- b) confirmar a identidade do solicitante e a validade da solicitação;
- c) Encaminhar a solicitação de emissão e de revogação de certificado à AC-JUS utilizando protocolo de comunicação seguro conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL[1]
- 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) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- j) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados, na forma dos itens 3.19, 3.1.10 e 3.1.11; e
- k) garantir que todas as aprovações técnicas de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas;

2.1.3. Obrigações do Titular do Certificado

As obrigações do titular de certificado 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 na PC AC-JUS;
- d) conhecer os seus direitos e obrigações, contemplados na PC da AC-JUS, 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 constantes do documento Leiaute de Certificados da AC-JUS; e
- g) operar de acordo com as regras e normas publicadas pela AC-JUS e ICP-Brasil.

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.

2.1.4.3. O não exercício desses direitos não afasta a responsabilidade da AC-JUS e do titular do certificado.



2.1.5. Obrigações do Repositório

O repositório da AC-JUS é mantido no ambiente do PSS, e possui recursos físicos, humanos e de infraestrutura computacional aptos a:

- a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC-JUS e a sua LCR;
- b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- c) implementar os recursos necessários para a segurança dos dados nele armazenados.

2.2. Responsabilidades

2.2.1. Responsabilidades da AC-JUS

2.2.1.1. A AC-JUS responderá pelos danos a que der causa.

2.2.1.2. A AC-JUS responderá solidariamente pelos atos das entidades de sua cadeia de certificação, AC subordinadas, AR e PSS.

2.2.2. Responsabilidades da AR

A AR-JUS será responsável pelos danos a que der causa.

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte usuária (Relying Party)

Não existe responsabilidade da terceira parte (parte confiante) perante AC emitente de um certificado ou AR a ela vinculada, exceto na prática de ato ilícito.

2.3.2. Relações Fiduciárias

A AC-JUS ou a AR-JUS indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3. Processos Administrativos

Será seguida a lei 9784 de 29 de janeiro de 1999 e qualquer outra legislação específica, uma vez que a AC-JUS e a AR-JUS são administradas pelo Conselho da Justiça Federal, órgão da Administração Pública Federal.

2.4. Interpretação e Execução

2.4.1. Legislação

A DPC AC-JUS obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001 e as Resoluções do CG da ICP-Brasil e as normas da AC-JUS.

2.4.2. Forma de interpretação e notificação



2.4.2.1. Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, o corpo técnico da AC-JUS examinará a disposição inválida e irá propor à Comissão Técnica, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada. As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.2.2. Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas na PC serão realizadas por iniciativa da AC-JUS por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil e às AC subseqüentes se for o caso.

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. Nesta situação 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 subseqüente 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 subseqüente 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

2.6.1.1. A AC-JUS publica e disponibiliza informações, tais como certificados, sua 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.

2.6.1.2. São publicados em página *web* da AC-JUS, <http://www.acjus.gov.br>:

- a) certificado da AC-JUS;
- b) sua LCR;
- c) esta DPC ;
- d) a PC que implementa;
- e) relação, regularmente atualizada contendo as AR vinculadas e seus endereços de instalações técnicas em funcionamento;
- f) relação, regularmente atualizada, das AR que tenham celebrado acordos operacionais com outras AR da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado;
- g) uma relação, regularmente atualizada dos PSS vinculados ;e
- h) o documento Leiaute do Certificado da AC-JUS, contendo o perfil dos certificados admitidos sob a 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. A LCR será publicada a cada 30 dias, no máximo, independentemente de haver alteração. Esta DPC AC-JUS, a PC AC-JUS e o Leiaute dos Certificados da AC-JUS são publicadas após aprovação pela AC Raiz da ICP-Brasil e sempre que sofrerem atualizações.

As demais informações mencionadas no item 2.6.1 serão publicadas sempre que sofrerem alterações.

2.6.3. Controles de acesso

O controle de acesso às informações publicadas pela AC-JUS obedece o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

Não há qualquer restrição ao acesso para consulta a esta DPC, à sua PC, aos certificados emitidos e à LCR da AC-JUS.

Acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso incluirão identificação pessoal para acesso aos equipamentos, utilização de senhas e utilização de protocolos seguros de comunicação de dados.

2.6.4. Repositórios

O repositório da AC-JUS está disponível para consulta e atende aos seguintes requisitos:

- a) localização: <http://www.acjus.gov.br/acjus/>;
- b) disponibilidade: aquela definida no item 2.6.1 desta DPC AC-JUS;
- c) protocolos de acesso: HTTP e HTTPS;
- d) requisitos de segurança de acordo com os requisitos definidos no item 5 desta DPC AC-JUS.



2.7. Fiscalização e Auditoria de conformidade

- 2.7.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.
- 2.7.2. As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICPBRASIL [2].
- 2.7.3. Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICPBRASIL [3].
- 2.7.4. A AC-JUS recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e que é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICPBRASIL [3].
- 2.7.5. As entidades da ICP-Brasil diretamente vinculadas à AR-JUS – AC, AR e PSS, também receberam auditoria prévia, para fins de credenciamento. A AC-JUS é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8. Sigilo

2.8.1. Disposições Gerais

- 2.8.1.1. A chave privada de assinatura digital da AC-JUS foi gerada e é mantida pela própria AC-JUS, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC-JUS é de sua inteira responsabilidade.
- 2.8.1.2. Os titulares de certificados emitidos pela AC-JUS, ou os responsáveis pelo seu uso, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, são responsáveis pela divulgação ou utilização indevidas dessas chaves.
- 2.8.1.3. Não se aplica.

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 LCR emitidos pela AC-JUS;



- b) informações corporativas ou pessoais que necessariamente façam parte dos certificados ou de diretórios públicos;
- c) as PC implementadas pela AC-JUS;
- d) a DPC da AC-JUS;
- e) versões públicas de Políticas de Segurança; e
- f) a conclusão dos relatórios de auditoria.

2.8.4. Divulgação de informação de revogação/suspensão de certificado

2.8.4.1. A AC-JUS disponibiliza em sua página <http://www.acjus.gov.br>, lista de certificados revogados. 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.

2.8.7. Divulgação por solicitação do titular

2.8.7.1. O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

2.8.7.2. Nenhuma liberação de informação é permitida sem autorização formal do titular do certificado, exceto nos casos do item 2.8.5. Autorizações formais podem ser apresentadas de duas formas:

- a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou
- b) por meio de pedido escrito com firma reconhecida.



2.8.8. Outras circunstâncias de divulgação de informação

Em nenhuma outra circunstância, que não esteja prevista nesta DPC, serão divulgadas informações sigilosas.

2.9. Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual inclusive os direitos autorais em todos os certificados e todos os documentos gerados para a AC-JUS (eletrônicos ou não), pertencem e continuarão sendo propriedade do Conselho da Justiça Federal.

Direitos sobre Identificadores de Objeto (OID) atribuídos à AC-JUS após o processo de credenciamento cabem única e exclusivamente ao Instituto de Tecnologia da Informação – ITI, operador da AC Raiz da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Registro Inicial

3.1.1. Disposições Gerais

3.1.1.1. A AR-JUS, vinculada à AC-JUS, utilizará os seguintes requisitos e procedimentos para a realização dos procedimentos que seguem:

- a) Validação da solicitação de certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:
 - i. confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado ou como representante legal de uma pessoa jurídica é realmente aquela cujos dados constam na documentação apresentada;
 - ii. confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;
 - iii. emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC;
- b) Verificação da solicitação de certificado – confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:
 - i. por agente de registro distinto do que executou a etapa de validação;
 - ii. em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;
 - iii. somente após o recebimento, na instalação técnica da AR, de cópia da documentação apresentada na etapa de validação;
 - iv. antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.1.1.2. O processo de validação poderá ser realizado pelo agente de registro fora do ambiente físico da AR, nesse caso será utilizado ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR, se for o caso.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado devem ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. Tais registros devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria



3.1.1.4. Deve ser 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].

3.1.2. Tipos de nomes

3.1.2.1. As AC de nível imediatamente subsequente ao da AC-JUS, titulares de certificados de AC habilitada, terão um nome que as identifique univocamente no âmbito da ICP-Brasil e da AC-JUS, no padrão ITU X.500.

- a) O DN (*Distinguished Name*) dos certificados deverá seguir o padrão definido no item 7.1.4.
- b) O atributo CN do DN deverá ser na forma:
“AC nomedaACsubseqüente-JUS”.

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.

3.1.8. Método para comprovar a posse de chave privada



A AC-JUS através de seus agentes de registro acompanham no ambiente off-line da AC candidata a subsequente, a geração do par de chaves e da solicitação do certificado (Certificate Request PKCS#10) contendo a chave pública correspondente à chave privada gerada. A solicitação é gravada em mídia, que é verificada e guardada em envelope lacrado. O envelope é então levado ao ambiente off-line da AC-JUS, onde é verificado quanto à violação e aberto na presença de representantes da AC-JUS, da AC candidata e de testemunhas do PSS da AC-JUS. A mídia é verificada novamente e é então utilizada no processo de emissão do certificado à AC subsequente.

3.1.9. Autenticação da Identidade de um Indivíduo

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

- a) Deverá ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de indivíduo solicitante de certificado:
- b) Cédula de Identidade ou Passaporte, se brasileiro;
- c) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
- d) Passaporte, se estrangeiro não domiciliado no Brasil;
- e) caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data da validação presencial;
- f) comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial; e
- g) mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4.

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

NOTA 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.9.2.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

- a) nome completo, sem abreviações;
- b) data de nascimento.

3.1.9.2.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

- a) Cadastro de Pessoa Física (CPF);
- b) número de Identificação Social NIS (PIS, PASEP ou CI);
- c) número do Registro Geral RG do titular e órgão expedidor;
- d) número do Cadastro Específico do INSS (CEI);



- e) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;
- f) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

3.1.9.2.3. Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original. Deve ser mantido arquivo com as cópias de todos os documentos utilizados.

NOTA 1: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

NOTA 2: O cartão CPF poderá ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.10. Autenticação da Identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.1.1. A confirmação da identidade de uma AC subordinada é feita com base no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL (DOC-ICP-03),

3.1.10.1.2. Será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

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;
- c) presença física do responsável pelo uso do certificado e assinatura do termo de responsabilidade de que trata o item 4.1.1; e
- d) presença física do(s) representante(s) legal(is) da pessoa jurídica 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

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. ato constitutivo, devidamente registrado no órgão competente; e
 - ii. 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 emitido para uma organização:

3.1.10.3.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

- a) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;
- b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
- c) nome completo do responsável pelo certificado, sem abreviações;



d) data de nascimento do responsável pelo certificado.

3.1.10.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de responsabilidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.1.9.2. (ITEM NÃO APLICÁVEL)

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Este item não se aplica uma vez que a AC-JUS emite somente certificados para AC subsequente.

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

Pode ser solicitado um novo certificado antes da expiração do atual, observando os mesmos requisitos e procedimentos exigidos para a solicitação de certificados.

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

Após a revogação de seu certificado, uma AC deve executar os processos regulares para geração de novo par de chaves.

3.4. Solicitação de Revogação

A solicitação de revogação de certificado de AC de nível imediatamente subsequente será feita formalmente pelo representante da AC, e com a presença física do mesmo **ou do responsável pelo uso certificado**, a fim de possibilitar a sua identificação inequívoca. A solicitação de revogação poderá ainda ser feita por decisão judicial, ou determinação da AC-Raiz.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado

4.1.1. A solicitação de emissão de um Certificado Digital para Autoridade Certificadora imediatamente subsequente à AC-JUS deverá ser feita através de documento formal do representante legal da AC candidata, o qual será submetido ao CG da AC-JUS para aprovação. Além da aprovação pelo CG, os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado são:

- a) A comprovação de atributos de identificação constantes do certificado;
- b) Não se aplica;
- c) um termo de titularidade assinado pelo titular do certificado e um termo de responsabilidade assinado pelo responsável pelo uso do certificado, estabelecendo as condições de uso deste, elaborados conforme os documentos MODELO DE TERMO DE TITULARIDADE [4] e MODELO DE TERMO DE RESPONSABILIDADE [5]

4.1.2. A solicitação de certificado para AC de nível imediatamente subsequente ao da AC-JUS somente é possível após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].



- 4.1.3. A AC subsequente deverá encaminhar a solicitação de seu certificado à AC-JUS por meio de seus representantes legais, utilizando padrão definido no documento PADRÕES E ALGORÍTMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]

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.
- 4.2.2. 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
- 4.2.3. A emissão dos certificados das AC de nível imediatamente subsequente à AC-JUS é feita em equipamentos que operam *off-line*.
- 4.2.4. A AC-JUS entrega o certificado emitido, no padrão definido no documento PADRÕES E ALGORÍTMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], para os representantes legais da AC habilitada.
- 4.2.5. 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. A AC titular tem o prazo de 2 (dois) dias úteis, contados do seu recebimento, para fazer a verificação dos dados do certificado. Após esse prazo o certificado é considerado aceito.
- 4.3.4. Ao aceitar o certificado, a AC titular:
- a) concorda com as responsabilidades, obrigações e deveres a ela impostos pelo Termo de Acordo e esta DPC.
 - b) garante que com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado
 - c) afirma que todas as informações de certificado fornecidas durante o processo de credenciamento são verdadeiras e estão reproduzidas no certificado de forma correta e completa.
 - d) aceita as regras e normas da AC-JUS para emissão de certificados na sua cadeia de certificação
- 4.3.5. A não aceitação do certificado dentro do prazo previsto implica na realização de nova cerimônia, onde é feita a revogação do certificado não aceito e a emissão de novo certificado.

4.4. Suspensão e Revogação de Certificado

4.4.1. Circunstâncias para revogação

- 4.4.1.1. Um certificado de AC de nível imediatamente subsequente ao da AC-JUS pode ser revogado a qualquer momento por solicitação da AC titular do certificado ou por decisão motivada da AC-JUS, ou da AC Raiz.
- 4.4.1.2. Um certificado é obrigatoriamente revogado:



- a) quando constatada emissão imprópria ou defeituosa;
- b) quando for necessária a alteração de qualquer informação constante no mesmo;
- c) no caso de dissolução da AC titular do certificado;
- d) no caso de comprometimento da chave privada da AC da sua mídia armazenadora; ou
- e) por decisão judicial.

4.4.1.3. Observa-se ainda que:

- a) A AC-JUS deverá revogar, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela AC-JUS ou da ICP-Brasil;
- b) O CG da ICP-Brasil ou a AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.4.2. Quem pode solicitar revogação

A revogação do certificado de uma AC de nível imediatamente subsequente ao da AC-JUS somente poderá ser solicitada:

- a) pela AC-JUS;
- b) pela AR-JUS;
- c) pela AC titular do certificado;
- d) pelo CG da ICP-Brasil;
- e) pela AC Raiz;
- f) por decisão judicial.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. A solicitação de revogação de certificado de AC subsequente deve ser feita através do formulário SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC [8]. Esse formulário deverá ser assinado pelo representante legal da AC. Se utilizada versão digital do documento, este deverá estar assinado digitalmente. Caso seja entregue em papel, o documento deverá ser entregue pessoalmente na AR-JUS pelo representante da AC subsequente, e assinado no ato da entrega.

4.4.3.2. Como diretrizes gerais, fica estabelecido que:

- a) O solicitante da revogação de um certificado será identificado;
- 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 são 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. O prazo para aceitação do certificado pelo titular é de 2 (dois) dias úteis, dentro desse prazo a revogação do certificado pode ser solicitada sem ônus.

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. Neste item é definida a frequência para a emissão de LCR referente a certificados de AC de nível imediatamente subsequente à AC JUS.

4.4.9.2. Não se aplica.

4.4.9.3. A frequência máxima admitida para emissão de LCR referente a certificados de AC imediatamente subsequente à AC-JUS é de 30 dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu a AC-JUS emitirá nova LCR no prazo previsto no item 4.4.3 e notificará todas as AC de nível imediatamente subsequente ao seu.

4.4.9.4. Não se aplica.

4.4.10. Requisitos para verificação de LCR

4.4.10.1. Todos os certificados revogados no domínio da AC-JUS são listados na LCR que pode ser acessada no endereço *web* contido no próprio certificado.

4.4.10.2. Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.

4.4.10.3. 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.

4.4.13. Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subsequente ao da AC-JUS poderão ser divulgadas por meio de sua publicação no Diário Oficial, Caderno III, Diário da Justiça e na página WEB da AC-JUS.

4.4.14. Requisitos para verificação de outras formas de divulgação de revogação

As formas de verificação descritas no item anterior são meramente informativas.

4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. No caso do comprometimento da chave privada de uma AC de nível imediatamente subsequente ao da AC-JUS, a mesma deve notificar imediatamente à AC-JUS.

4.4.15.2. A comunicação do comprometimento da chave privada de uma AC poderá ser feita, por correio eletrônico assinado digitalmente pelo representante legal da AC.

4.5. Procedimentos de Auditoria de Segurança

4.5.1. Tipos de Evento Registrados

4.5.1.1. A AC-JUS registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

- a) iniciação e desligamento do sistema de certificação;
- b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC-JUS;
- c) mudanças na configuração da AC-JUS ou nas suas chaves;
- d) mudanças nas políticas de criação de certificados;
- e) tentativas de acesso (*login*) e de saída do sistema (*logout*);
- f) tentativas não autorizadas de acesso aos arquivos de sistema;
- g) geração de chaves próprias da AC-JUS ou de chaves de Titulares de Certificados;
- h) emissão e revogação de certificados;
- i) geração de LCR;
- j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
- k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
- l) operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A AC-JUS registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, quais sejam:



-
- | | |
|----|--|
| a) | Registros de acessos físicos; |
| b) | Manutenção e mudanças na configuração de seus sistemas; |
| c) | Mudanças de pessoal e de perfis qualificados; |
| d) | Relatórios de discrepância e comprometimento; e |
| e) | Registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários. |

4.5.1.3. Os registros de auditoria mínimos a serem mantidos pela AC-JUS incluem além dos acima:

- | | |
|----|--|
| a) | Registros de solicitação, inclusive registros relativos a solicitações rejeitadas; |
| b) | Pedidos de geração de certificado, mesmo que a geração não tenha êxito; |
| c) | Registros de solicitação de emissão de LCR. |

4.5.1.4. Todo o registro de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a identidade do agente que o causou.

4.5.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC-JUS é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil[8].

4.5.1.6. 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 <i>log-in</i> e <i>log-out</i>	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
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados	Automático	AC ou Software de AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado	Automático	Software de AR
Logs de <i>Backup</i> e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de <i>software</i> e <i>hardware</i>	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	Software de controle de acesso e pessoal de operações



4.5.7. Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC-JUS não são notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8. Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a AC-JUS. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação.

Eventos que indiquem possível vulnerabilidade, detectados na análise dos registros de auditoria da AC-JUS, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

4.6. Arquivamento de Registros

4.6.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC-JUS:

- a) solicitações de certificados;
- b) solicitações de revogação de certificados;
- c) notificações de comprometimento de chaves privadas;
- d) emissões e revogações de certificados;
- e) emissões de LCR;
- f) trocas de chaves criptográficas da AC-JUS;
- g) informações de auditoria previstas no item 4.5.1;
- h) correspondências formais;
- i) Processos de credenciamento de AC de nível imediatamente subsequente ao da AC-JUS.

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 30 anos a contar da data de expiração ou revogação do certificado;e
- c) as demais informações, inclusive registros de auditoria são retidas por, no mínimo, 6 (seis) 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 contém 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	Automático e manual	Software de AC/AR e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados	Automático	Software de AC/AR
Emissões de LCR	Automático	Software de AC/AR
Correspondências formais	Manual	Pessoal de operações

4.6.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC-JUS, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado. Não serão disponibilizadas informações sigilosas para verificação.

4.7. Troca de chave

- 4.7.1. A AC de nível imediatamente subsequente ao da AC-JUS deverá iniciar, até 90 dias antes da expiração do seu certificado, o processo de geração de novo par de chaves e de emissão de novo certificado.
- 4.7.2. Uma vez expirado o certificado de uma AC de nível imediatamente subsequente ao seu a AC-JUS remove imediatamente esse certificado do diretório e de sua página WEB, mantendo-o armazenado permanentemente para efeito de consulta histórica



4.8. Comprometimento e Recuperação de Desastre

Os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres estão descritos no PCN da AC-JUS, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

4.8.1. Recursos computacionais, software ou dados corrompidos

A AC-JUS possui um Plano de Continuidade de Negócio – PCN, de caráter sigiloso, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos.

O PCN especifica as ações a serem tomadas no caso em que recursos computacionais, *software* e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

- a) É feita a identificação de todos os elementos corrompidos;
- b) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
- c) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um *backup* de segurança até a revogação do certificado da AC-JUS.

4.8.2. Certificado de entidade revogado

A AC-JUS possui um Plano de Continuidade de Negócio – PCN de caráter sigiloso, que especifica as ações a serem tomadas no caso em que o certificado da AC-JUS for revogado. Que se resumem no seguinte:

- a) Em caso de revogação do certificado da AC-JUS, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora.
- b) A seguir são revogados os certificados das AC de nível imediatamente subsequente. É gerado novo par de chaves da AC-JUS, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado. A AC-JUS, emite então novos certificados digitais para as AC de nível imediatamente subsequente.

4.8.3. Chave de entidade comprometida

A AC-JUS possui um PCN que especifica as ações a serem tomadas no caso em que a chave privada da AC-JUS for comprometida, e que se resumem no seguinte:

- a) Em caso de comprometimento da chave da AC-JUS, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora.
- b) Na confirmação do incidente, são revogados os certificados da AC-JUS e das AC de nível imediatamente subsequente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-JUS, novos certificados digitais para as AC de nível imediatamente subsequente.

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 possui um PCN onde são descritos os procedimentos previstos para recuperação total ou parcial das atividades da AR-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 prevaletentes, 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

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.

5.1.1.1.2. Todas as instalações da AC-JUS, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos a seguir:

- a) Todas as instalações de equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, retificadores, estabilizadores e similares;
- b) instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas;
- c) iluminação de emergência.

5.1.2. Acesso físico

O acesso físico às dependências da AC-JUS é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso.

O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes.

O sistema de certificação da AC-JUS está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.3. Níveis de Acesso

5.1.3.1.1. São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC-JUS, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

5.1.3.1.1.2. **O primeiro nível – ou nível 1**– Situa-se após a primeira barreira de acesso às instalações da AC-JUS. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC-JUS transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC-JUS é executado nesse nível.

5.1.3.1.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC-JUS, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *paggers*, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.3.1.1.4. **O segundo nível – ou nível 2**– é interno ao primeiro nível. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas por meio eletrônico, e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC-JUS.

5.1.3.1.1.5. **O terceiro nível – ou nível 3**– é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC-JUS. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não

estejam envolvidas com essas atividades não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

- 5.1.3.1.6. No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual, como cartão eletrônico, e a identificação biométrica.
- 5.1.3.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC-JUS, não são admitidos a partir do nível 3.
- 5.1.3.1.8. **O quarto nível - ou nível 4** – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da AC-JUS, tais como: emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.
- 5.1.3.1.9. 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.
- 5.1.3.1.10. A sala cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.
- 5.1.3.1.11. 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 infra-estrutura (firewall, roteadores, switches e servidores)
- 5.1.3.1.12. **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.
- 5.1.3.1.13. 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.
- 5.1.3.1.14. **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

5.1.3.2. Sistema físico de detecção

- 5.1.3.2.1. 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.
- 5.1.3.2.2. 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.

- 5.1.3.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes.
- 5.1.3.2.4. 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.
- 5.1.3.2.5. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.
- 5.1.3.2.6. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmaras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.4. Sistema de Controle de Acesso

O sistema de controle de acesso está baseado em um ambiente de nível 4.

5.1.5. Mecanismos de emergência

- 5.1.5.1.1. Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC-JUS em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.
- 5.1.5.1.2. Todos os procedimentos referentes aos mecanismos de emergência estão documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.6. Energia e ar condicionado

- 5.1.6.1. A infraestrutura do ambiente de certificação da AC-JUS é dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC-JUS e seus respectivos serviços. Um sistema de aterramento está implantado;
- 5.1.6.2. Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados;
- 5.1.6.3. São utilizadas tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, de telefonia e de dados;
- 5.1.6.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.
- 5.1.6.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8]. Qualquer modificação nessa rede é previamente documentada.



-
- 5.1.6.6. Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.
 - 5.1.6.7. O sistema de climatização atende aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante à falhas.
 - 5.1.6.8. A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.
 - 5.1.6.9. O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.
 - 5.1.6.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC é garantida por meio de:
 - a) Geradores de porte compatível;
 - b) Geradores de reserva, do mesmo porte dos citados no nível 1;
 - c) Sistemas de “no-breaks” redundantes;
 - d) Sistemas redundantes de ar condicionado.

5.1.7. Exposição à água

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.

5.1.8. Prevenção e proteção contra incêndio

- 5.1.8.1. 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 sobre-aquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.
- 5.1.8.2. Nas instalações da AC-JUS não é permitido fumar ou portar objetos que produzam fogo ou faísca.
- 5.1.8.3. 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 esta fechada.
- 5.1.8.4. 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.

5.1.9. Armazenamento de mídia

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

5.1.10. Destruição de lixo

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



5.1.11. 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.

5.1.12. Instalações Técnicas de AR

Não se aplica.

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

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.

- 5.2.1.1. 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.

5.2.2. Número de pessoas necessário por tarefa

- 5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC-JUS, conforme o descrito em 6.2.2.
- 5.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC-JUS necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC-JUS.

5.2.3. Identificação e autenticação para cada perfil

Pessoas que ocupam os perfis designados pela AC-JUS passam por um processo rigoroso de seleção. Todo funcionário da AC-JUS tem sua identidade e perfil verificados antes de:

- a) Ser incluído em uma lista de acesso às instalações da AC-JUS;



-
- | | |
|----|--|
| b) | ser incluído em uma lista para acesso físico ao sistema de certificação da AC-JUS; |
| c) | receber um certificado para executar suas atividades operacionais na AC-JUS; |
| d) | receber uma conta no sistema de certificação da AC-JUS. |

5.2.3.1. Os certificados, contas e senhas utilizados para identificação e autenticação dos funcionários:

- a) São diretamente atribuídos a um único operador (funcionário da AC-JUS devidamente qualificado);
- b) não são compartilhados;
- c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.2. A AC-JUS implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC-JUS, pelas AR e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os empregados da AC-JUS e das AR e PSS vinculados, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- | | |
|----|---|
| a) | Os termos e as condições do perfil que ocupam. |
| b) | O compromisso de observar as normas, políticas e regras aplicáveis da AC-JUS. |
| c) | O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil. |
| d) | O compromisso de não divulgar informações sigilosas a que tenham acesso. |

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC-JUS envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC-JUS e na Política de Segurança da ICP-Brasil[8].

5.3.2. Procedimentos de Verificação de Antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade da AC-JUS, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é submetido aos seguintes processos, antes do começo das atividades de:

- a) Verificação de antecedentes criminais;
- b) Verificação de situação de crédito;
- c) Verificação de histórico de empregos anteriores;
- d) Comprovação de escolaridade e de residência;
- e) Caso servidor público, histórico de processos administrativos.



5.3.3. Requisitos de treinamento

Todo o pessoal da AC-JUS e das AR vinculadas, 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 das AR's vinculadas 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 toma 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 operandis*";
- 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 ICP-Brasil.



5.3.7. Requisitos para contratação de pessoal

O pessoal da AC-JUS, das AR Vinculadas, 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 na Política de Segurança da ICP Brasil[8].

5.3.8. Documentação disponibilizada ao pessoal

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

- a) esta DPC;
- b) a PC que implementa;
- c) a Política de Segurança da ICP-Brasil;
- d) a Política de Segurança da AC-JUS;
- e) documentação de hardware e software relativa à função desempenhada;
- f) documentação operacional relativa às suas atividades; e
- g) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de chaves

6.1.1. Geração do Par de Chaves

6.1.1.1. O par de chaves da AC-JUS é gerado pela própria AC-JUS, em módulo criptográfico de hardware com padrão de segurança FIPS 140-1 level 3 ou superior, utilizando algoritmo RSA para geração do par de chaves e algoritmo 3-DES para sua proteção, após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. O par de chaves criptográficas de uma AC de nível imediatamente subsequente ao da AC-JUS é gerado pela própria AC solicitante, após o deferimento do pedido de credenciamento e habilitação da mesma, e a consequente autorização de funcionamento no âmbito da ICP-Brasil. O par de chaves deverá ser gerado e a chave privada armazenada, em hardware criptográfico aprovado pelo CG da ICP-Brasil.

6.1.1.3. As PC implementadas pela AC-JUS e pelas AC subordinadas definem o meio utilizado para armazenamento das respectivas chaves privadas, com base nos requisitos aplicáveis estabelecidos pelo documento Requisitos Mínimos para Políticas de Certificado na ICP-Brasil[7].

6.1.2. Entrega da chave privada à entidade titular

Não se aplica.

É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.



6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC-JUS fará uso do padrão PKCS#10, em data e hora previamente estabelecidos pela AC-Raiz da ICP-Brasil.

6.1.3.2. Para a entrega de sua chave pública à AC-JUS, encarregada da emissão de seu certificado, a AC solicitante faz uso do padrão PKCS#10. Essa entrega é feita por representante legalmente constituído da AC subordinada, em data e hora acordada entre as partes.

6.1.4. Disponibilização de chave pública da AC-JUS para usuários

As formas para a disponibilização do certificado da AC-JUS, e de todos os certificados da cadeia de certificação, para os usuários da AC-JUS, compreendem:

- a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9];
- b) diretório;
- c) página web da AC-JUS (<http://www.acjus.gov.br>);
- d) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho das chaves criptográficas associadas a certificados emitidos pela AC-JUS seguirá o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC-JUS seguem o padrão FIPS (*Federal Information Processing Standards*) 140-11 *level 3* ou superior, uma vez que utilizam *hardware* criptográfico com esta certificação. Este padrão está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7. Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave é feita de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*), uma vez que o *hardware* utilizado é certificado pelo NIST como FIPS 140-1 *level 3* ou superior. Este padrão é definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8. Geração de chave por hardware ou software

1 FIPS 140-1 – *Federal Information Processing Standards* 140-1. Esse padrão será substituído pelo FIPS 140-2, hoje em fase de implantação por parte do National Institute of Standards and Technology.



6.1.8.1. O processo de geração do par de chaves da AC-JUS é feito por hardware padrão FIPS (Federal Information Processing Standards) 140-1, level 3.

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 certificado emitidos pela AC-JUS poderão ser utilizada 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.

6.1.10. Proteção da Chave Privada

A chave privada da AC-JUS é gerada, armazenada e utilizada apenas em hardware criptográfico específico, classificado como FIPS 140-1 level 3, não havendo, portanto, tráfego da mesma em nenhum momento.

6.1.11. Padrões para módulo criptográfico

6.1.11.1. 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 classificado como FIPS 140-1 Nível 3. Este padrão é definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.11.2. O padrão requerido para os módulos de geração de chaves criptográficas das AC de nível imediatamente subsequente ao da AC-JUS é o FIPS 140-1 Nível 2 ou superior.

6.1.12. Controle “n de m’ para chave privada

6.1.12.1. 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).

6.1.12.2. É necessária a presença de no mínimo “2” custodiantes (n) para a ativação do componente e a consequente utilização da chave privada.

6.1.13. 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.

6.1.14. Cópia de segurança (backup) de chave privada

6.1.14.1. Como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.1.14.2. 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.

6.1.14.3. A AC-JUS não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.

6.1.14.4. A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+, ou outros definidos no documento. Este padrão é definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.15. Arquivamento de chave privada

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

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

6.1.16. Inserção de chave privada em módulo criptográfico

A chave privada da AC-JUS é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.1.17. Método de ativação de chave privada

A ativação da chave privada da AC-JUS é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de “2” de “9” dos *custodiantes* da chave de ativação da chave criptográfica. Os *custodiantes* da chave privada serão magistrados ou servidores do Poder Judiciário Federal indicados pelo Comitê Gestor da AC-JUS. As senhas obedecem à política de senhas estabelecida pela AC-JUS.

6.1.18. Método de desativação de chave privada

A chave privada da AC-JUS, armazenada em módulo criptográfico é desativada, quando não mais necessária, através de mecanismo disponibilizado pelo software de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de “2” de “9” dos *custodiantes* da chave de ativação da chave criptográfica. As senhas obedecem à política de senhas estabelecida pela AC-JUS.

6.1.19. Método de destruição de chave privada

Quando a chave privada da AC-JUS for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, deve ser sobrescrito. Todas as cópias de segurança da chave privada da AC-JUS e os cartões criptográficos dos *custodiantes* serão destruídos. Os agentes autorizados para realizar estas operações são os administradores e os *custodiantes* das chaves de ativação da AC-JUS.

6.2. Outros Aspectos do Gerenciamento do Par de Chaves

6.2.1. Arquivamento de chave pública



As chaves públicas da própria AC-JUS, e dos titulares dos certificados por ela emitidos, bem como as LCR emitidas, serão armazenados pela AC-JUS, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.2.2. Períodos de uso para as chaves pública e privada

6.2.2.1. A chave privada da AC-JUS bem como as chaves privadas dos titulares dos certificados por ela emitidos, deverão ser utilizadas apenas durante o período de validade do certificado correspondente. 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 do certificado correspondente.

6.2.2.2. Não se aplica.

6.2.2.3. A PC implementada define o período máximo de validade dos certificados emitidos pela AC-JUS, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.2.2.4. Os certificados emitidos pela AC-JUS para as AC's de nível imediatamente subsequente ao seu terão validade de no máximo 8 (oito) anos.

6.3. Dados de ativação

6.3.1. Geração e instalação dos dados de ativação

6.3.1.1. Os dados de ativação da chave privada da AC-JUS são únicos e aleatórios.

6.3.1.2. Não se aplica.

6.3.2. Proteção dos dados de ativação.

6.3.2.1. Os dados de ativação são protegidos por cartões criptográficos individuais com senha, e são armazenados em ambiente de nível 6 de segurança.

6.3.2.2. Não se aplica.

6.3.3. Outros aspectos dos dados de ativação

Não se aplica.

6.4. Controles de Segurança dos computadores

6.4.1. Requisitos técnicos específicos de segurança computacional

6.4.1.1. 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.

6.4.1.2. 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.



6.4.1.3. Os computadores servidores, utilizados pela AC-JUS e pelas AC subordinadas, 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) Acesso restrito aos bancos de dados da AC-JUS;
- d) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- e) Geração e armazenamento de registros de auditoria da AC-JUS;
- f) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- g) Mecanismos para cópias de segurança (*backup*).

6.4.1.4. Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.

6.4.1.5. 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.

6.4.1.6. 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.

6.4.2. 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.

6.4.3. Controle de segurança para as Autoridades de Registro

6.4.3.1. Não se aplica.

6.4.3.2. Não se aplica.

6.5. Controles Técnicos do Ciclo de Vida

6.5.1. Controles de desenvolvimento de sistemas

6.5.1.1. A AC-JUS adota sistema de certificação do SERPRO (Serviço Federal de Processamento de



Dados), desenvolvido em código aberto, todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após a conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do CCD avalia e após consultar a AC-JUS, decide quando será a implementação no ambiente de produção.

- 6.5.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC-JUS ou seu PSS proverão documentação suficiente para suportar avaliações externas de segurança dos componentes da AC-JUS.

6.5.2. Controle de gerenciamento de segurança

6.5.2.1. As ferramentas e os procedimentos empregados pela AC-JUS para garantir que os seus sistemas implementem os níveis configurados de segurança são os seguintes:

- a) A AC-JUS opera em equipamento off-line, portanto não necessita configuração de segurança de rede.
- b) A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

6.5.2.2. O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC-JUS, envolve o teste de mudanças planejadas no Ambiente de Desenvolvimento e Homologação isolados antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

- a) Instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
- b) Implantação ou modificação de Autoridades Certificadoras com customizações de certificados, páginas web, scripts, etc.;
- c) Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e
- d) Instalação de novos serviços na plataforma de processamento.

6.5.3. Classificação de segurança de ciclo de vida

Não se aplica.

6.6. Controles de Segurança de Rede

6.6.1. Diretrizes Gerais

6.6.1.1. Neste item são descritos os controles relativos à segurança da rede da AC responsável, incluindo firewalls e recursos similares.

6.6.1.2. Nos servidores do sistema de certificação AC-JUS, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

6.6.1.3. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC, estão localizados e operam em ambiente de nível, no mínimo, 4.

6.6.1.4. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (patches), disponibilizadas pelos respectivos fabricantes serão implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

6.6.1.5. O acesso lógico aos elementos de infraestrutura e proteção de rede deverão 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.

6.6.2. Firewall

6.6.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Um firewall promove o isolamento, em subredes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC.

6.6.2.2. O software de firewall, entre outras características, implementa registros de auditoria.

6.6.3. Sistema de detecção de intrusão (IDS)

6.6.3.1. O sistema de detecção de intrusão têm capacidade de 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 email 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.

6.6.3.2. O sistema de detecção de intrusão têm capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

6.6.3.3. 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.

6.6.4. Registro de acessos não autorizados à rede

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

6.7. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela AC-JUS para o armazenamento de sua chave privada é certificado como FIPS (*Federal Information Processing Standards*) 140-1, level 3.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico em concordância com os padrões aprovados 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.

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.

7.1.2. Não se aplica.

7.1.3. Nos itens seguintes está especificados o formato dos certificados emitidos pela AC-JUS.

7.2. Perfil do Certificado

Todos os certificados emitidos pela AC-JUS estão em conformidade com o formato definido pelo padrão ITU X.509.

7.2.1. Número(s) de versão

Todos os certificados emitidos pela AC-JUS implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

7.2.2. Extensões de certificados

Os certificados emitidos pela AC-JUS, sob a PC AC-JUS, obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

- a) “*Authority Key Identifier*”, não crítica: o campo `keyIdentifier` contém o resumo (hash) SHA-1 da chave pública da AC-JUS;
- b) “*Subject Key Identifier*”, não crítica: contém o *hash* SHA-1 da chave pública da AC titular do certificado;
- c) “*Key Usage*”, crítica: somente os bits `keyCertSign` e `cRLSign` são ativados;
- d) “*Certificate Policies*”, não crítica:
 - i. o campo `policyIdentifier` contém o OID das PC que a AC titular do certificado implementa;
 - ii. o campo `policyQualifiers` contém o endereço *URL* da página *web*, <http://www.acjus.gov.br/acjus/dpcacjus.pdf>, onde se obtém a DPC da AC-JUS;
- e) o campo “*Basic Constraints*”, crítica: contém o campo `CA=TRUE`;
- f) “*CRL Distribution Points*”, não crítica: contém o endereço *URL* da página *web* onde se obtém a LCR da AC-JUS.



7.2.3. Identificadores de algoritmos

Os certificados emitidos pela AC-JUS são assinados com o uso do algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

7.2.4. Formatos de nome

Para os certificados emitidos sob a PC 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

CN= nome da AC titular

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

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
\$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40



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 **2.16.76.1.1.1.9**.

7.2.7. Uso da extensão “Policy Constraints”

A extensão “Policy Constraints” poderá ser utilizada, da forma definida na RFC 3280, 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* da DPC da AC-JUS.

7.2.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas, no âmbito da AC-JUS, conforme a RFC 3280.

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 3280.

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:

- “*Authority Key Identifier*”: contém o hash SHA-1 da chave pública da AC-JUS que assina a LCR.
- “*CRL Number*”, não crítica: contém número sequencial 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 do CG da ICP-Brasil. A DPC será alterada sempre que uma nova PC implementada o exigir.

8.2. Políticas de publicação e de notificação

A AC-JUS publica esta DPC, em sua página *web*, acessível pela URL <http://www.acjus.gov.br/acjus/dpcacjus.pdf>. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na *web*.



8.3. Procedimentos de aprovação

Esta DPC foi submetida à aprovação da AC-RAIZ da ICP-Brasil, durante o processo de credenciamento da AC-JUS, conforme o determinado pelo documento “Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil[6]”.

9. DOCUMENTOS REFERENCIADOS

- 9.1. Os documentos listados a seguir 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
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

- 9.2. Os documentos a seguir 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]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

- 9.3. Os documentos abaixo 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
-----	-------------------	--------



Autoridade Certificadora da Justiça
Declaração de Práticas de Certificação
DPC AC-JUS

[4]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.A
[5]	MODELO DE TERMO DE RESPONSABILIDADE	ADE-ICP-05.B