

Declaração de Práticas de Certificação
Autoridade Certificadora
da Justiça

(DPC AC-JUS)

OID 2.16.76.1.1.19
Versão 10
Outubro 2026

1. INTRODUÇÃO 13
1.1. Visão Geral 13
1.2. Nome do documento e identificação 13
1.3. Participantes da ICP-Brasil 13
1.3.1. Autoridades Certificadoras 13
1.3.2. Autoridades de Registro 13
1.3.3. Titulares de Certificado 13
1.3.4. Partes Confiáveis 13
1.3.5. Outros participantes 14
1.4. Usabilidade do Certificado 14
1.4.1. Uso apropriado do Certificado 14
1.4.2. Uso proibitivo do Certificado 14
1.5. Política de Administração 14
1.5.1. Organização administrativa do documento 14
1.5.2. Contatos 14
1.5.3. Pessoa que determina a adequabilidade da DPC para a política 14
1.5.4. Procedimentos de aprovação da DPC 14
1.6. Definições e Acrônimos 14
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 16
2.1. Repositórios 16
2.2. Publicação de informações dos certificados 17
2.3. Tempo ou frequência de publicação 17
2.4. Controles de acesso aos repositórios 17
3. IDENTIFICAÇÃO E AUTENTICAÇÃO 17
3.1. Atribuição de Nomes 17
3.1.1. Tipos de nomes 17
3.1.2. Necessidade de nomes serem significativos 17
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado 17
3.1.4. Regras para interpretação de vários tipos de nomes 18
3.1.5. Unicidade de nomes 18
3.1.6. Procedimento para resolver disputa de nomes 18

3.1.7. Reconhecimento, autenticação e papel de marcas registradas 18
3.2. Validação Inicial de Identidade 18
3.2.1. Método para comprovar o controle de chave privada 18
3.2.2. Autenticação da Identidade de uma organização 19
3.2.3. Autenticação da Identidade de um indivíduo 19
3.2.4. Informações não verificadas do titular do certificado 20
3.2.5. Validação das Autoridades 20
3.2.6. Critérios para interoperabilidade 20
3.2.7. Autenticação da identidade de equipamento ou aplicação 20
3.3. Identificação e autenticação para pedidos de novas chaves 20
3.4. Identificação e Autenticação para solicitação de revogação 21
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 21
4.1. Solicitação de Certificado 21
4.1.1. Quem pode submeter uma solicitação 21
4.1.2. Processo de registro e responsabilidades 21
4.2. Processamento de Solicitação de Certificado 23
4.2.1. Execução das funções de identificação e autenticação 23
4.2.2. Aprovação ou rejeição de pedidos de certificado 23
4.2.3. Tempo para processar a solicitação de certificado 23
4.3. Emissão de Certificado 23
4.3.1. Ações da AC durante a emissão de um certificado 23
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado 23
4.4. Aceitação de Certificado 23
4.4.1. Conduta sobre a aceitação do certificado 23
4.4.2. Publicação do certificado pela AC 24
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades 24
4.5. Usabilidade do par de chaves e do certificado 24
4.5.1. Usabilidade da Chave privada e do certificado do titular 24
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis 24
4.6. Renovação de Certificados 24
4.6.1. Circunstâncias para renovação de certificados 24

4.6.2. Quem pode solicitar a renovação 24
4.6.3. Processamento de requisição para renovação de certificados 24
4.6.4. Notificação para nova emissão de certificado para o titular 24
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado 24
4.6.6. Publicação de uma renovação de um certificado pela AC 25
4.6.7. Notificação de emissão de certificado pela AC para outras entidades 25
4.7. Nova chave de certificado (Re-key) 25
4.7.1. Circunstâncias para nova chave de certificado 25
4.7.2. Quem pode requisitar a certificação de uma nova chave pública 25
4.7.3. Processamento de requisição de novas chaves de certificado 25
4.7.4. Notificação de emissão de novo certificado para o titular 25
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada 25
4.7.6. Publicação de uma nova chave certificada pela AC 25
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades 25
4.8. Modificação de certificado 25
4.8.1. Circunstâncias para modificação de certificado 25
4.8.2. Quem pode requisitar a modificação de certificado 25
4.8.3. Processamento de requisição de modificação de certificado 25
4.8.4. Notificação de emissão de novo certificado para o titular 25
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado 25
4.8.6. Publicação de uma modificação de certificado pela AC 25
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades 25
4.9. Suspensão e Revogação de Certificado 26
4.9.1. Circunstâncias para revogação 26
4.9.2. Quem pode solicitar revogação 26
4.9.3. Procedimento para solicitação de revogação 26
4.9.4. Prazo para solicitação de revogação 27
4.9.5. Tempo em que a AC deve processar o pedido de revogação 27
4.9.6. Requisitos de verificação de revogação para as partes confiáveis 27
4.9.7. Frequência de emissão de LCR 27
4.9.8. Latência máxima para a LCR 27

4.9.9. Disponibilidade para revogação/verificação de status on-line....27
4.9.10. Requisitos para verificação de revogação on-line....27
4.9.11. Outras formas disponíveis para divulgação de revogação....27
4.9.12. Requisitos especiais para o caso de comprometimento de chave....28
4.9.13. Circunstâncias para suspensão....28
4.9.14. Quem pode solicitar suspensão....28
4.9.15. Procedimento para solicitação de suspensão....28
4.9.16. Limites no período de suspensão....28
4.10. Serviços de status de certificado....28
4.10.1. Características operacionais....28
4.10.2. Disponibilidade dos serviços....28
4.10.3. Funcionalidades operacionais....28
4.11. Encerramento de atividades....28
4.12. Custódia e recuperação de chave....29
4.12.1. Política e práticas de custódia e recuperação de chave....29
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão....29
5. Controles Operacionais , Gerenciamento e de Instalações....29
5.1. Controle Físico....29
5.1.1. Construção e localização das instalações de AC....29
5.1.2. Acesso físico nas instalações de AC....29
5.1.3. Energia e ar condicionado nas instalações de AC....31
5.1.4. Exposição à água nas instalações de AC....32
5.1.5. Prevenção e proteção contra incêndio nas instalações de AC....32
5.1.6. Armazenamento de mídia nas instalações de AC....32
5.1.7. Destruição de lixo nas instalações de AC....32
5.1.8. Instalações de segurança (backup) externas (off-site)....33
5.2. Controles Procedimentais....33
5.2.1. Perfis qualificados....33
5.2.2. Número de pessoas necessário por tarefa....33
5.2.3. Identificação e autenticação para cada perfil....33
5.2.4. Funções que requerem separação de deveres....34

5.3. Controles de Pessoal 34
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade 34
5.3.2. Procedimentos de Verificação de Antecedentes 34
5.3.3. Requisitos de treinamento 34
5.3.4. Frequência e requisitos para reciclagem técnica 34
5.3.5. Frequência e sequência de rodízios de cargos 35
5.3.6. Sanções para ações não autorizadas 35
5.3.7. Requisitos para contratação de pessoal 35
5.3.8. Documentação fornecida ao pessoal 35
5.4. Procedimentos de Auditoria de Segurança 35
5.4.1. Tipos de Evento Registrados 35
5.4.2. Frequência de auditoria de registros (logs) 36
5.4.3. Período de Retenção para registros (logs) de Auditoria 36
5.4.4. Proteção de registro (log) de Auditoria 36
5.4.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria 37
5.4.6. Sistema de coleta de dados de auditoria 37
5.4.7. Notificação de agentes causadores de eventos 37
5.4.8. Avaliações de vulnerabilidade 37
5.5. Arquivamento de Registros 38
5.5.1. Tipos de registros arquivados 38
5.5.2. Período de retenção para arquivo 38
5.5.3. Proteção de arquivos 38
5.5.4. Procedimentos para cópia de arquivos 38
5.5.5. Requisitos para datação de registros 38
5.5.6. Sistema de coleta de dados de arquivo 38
5.5.7. Procedimentos para obter e verificar informação de arquivo 39
5.6. Troca de chave 39
5.7. Comprometimento e Recuperação de Desastre 39
5.7.1. Procedimentos gerenciamento de incidente e comprometimento 39
5.7.2. Recursos computacionais, software ou dados corrompidos 39
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade 39

5.7.4. Capacidade de continuidade de negócio após desastre....40
5.8. Extinção dos serviços de AC-JUS ou PSS....40
6. Controles Técnicos de Segurança....40
6.1. Geração e Instalação do Par de chaves....40
6.1.1. Geração do Par de Chaves....40
6.1.2. Entrega da chave privada à entidade titular....41
6.1.3. Entrega da chave pública para emissor de certificado....41
6.1.4. Entrega da chave pública da AC às terceiras partes....41
6.1.5. Tamanhos de chave....41
6.1.6. Geração de parâmetros de chaves assimétricas....41
6.1.7. Propósitos de uso de chave (conforme campo "Key usage" na X.509 v3)....42
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico....42
6.2.1. Padrões e controle para módulo criptográfico....42
6.2.2. Controle "n de m' para chave privada....42
6.2.3. Recuperação (escrow) de chave privada....42
6.2.4. Cópia de segurança de chave privada....42
6.2.5. Arquivamento de chave privada....42
6.2.6. Inserção de chave privada em módulo criptográfico....42
6.2.7. Armazenamento de chave privada em módulo criptográfico....43
6.2.8. Método de ativação de chave privada....43
6.2.9. Método de desativação de chave privada....43
6.2.10. Método de destruição de chave privada....43
6.3. Outros Aspectos do Gerenciamento do Par de Chaves....43
6.3.1. Arquivamento de chave pública....43
6.3.2. Períodos de uso para as chaves pública e privada....43
6.4. Dados de ativação....43
6.4.1. Geração e instalação dos dados de ativação....43
6.4.2. Proteção dos dados de ativação....43
6.4.3. Outros aspectos dos dados de ativação....44
6.5. Controles de Segurança Computacional....44
6.5.1. Requisitos técnicos específicos de segurança computacional....44

6.5.2. Classificação da segurança computacional 44
6.5.3. Controle de segurança para as Autoridades de Registro 44
6.6. Controles Técnicos do Ciclo de Vida 45
6.6.1. Controles de desenvolvimento de sistemas 45
6.6.2. Controle de gerenciamento de segurança 45
6.6.3. Classificação de segurança de ciclo de vida 45
6.6.4. Controles na Geração de LCR 45
6.7. Controles de Segurança de Rede 45
6.7.1. Diretrizes Gerais 45
6.7.2. Firewall 46
6.7.3. Sistema de detecção de intrusão 46
6.7.4. Registro de acessos não autorizados à rede 47
6.8. Carimbo de Tempo 47
7. Perfis de Certificado e LCR 47
7.1. Perfil do Certificado 47
7.1.1. Número(s) de versão 47
7.1.2. Extensões de certificados 47
7.1.3. Identificadores de algoritmos 48
7.1.4. Formatos de nome 48
7.1.5. Restrições de nome 48
7.1.6. OID (Object Identifier) de DPC 49
7.1.7. Uso da extensão “Policy Constraints” 49
7.1.8. Sintaxe e semântica dos qualificadores de política 49
7.1.9. Semântica de processamento para extensões criticas 49
7.2. Perfil de LCR 49
7.2.1. Número (s) de versão 49
7.2.2. Extensões de LCR e de suas entradas 49
7.3. Perfil de OCSP 49
7.3.1. Número(s) de versão 50
7.3.2. Extensões de OCSP 50
8. Auditoria de conformidade de outras avaliações 50

8.1. Frequência e circunstâncias das avaliações 50
8.2. Identificação/Qualificação do avaliador 50
8.3. Relação do avaliador com a entidade avaliada 50
8.4. Tópicos cobertos pela avaliação 50
8.5. Ações tomadas como resultado de uma deficiência 50
8.6. Comunicação dos resultados 50
9. Outros Negócios e assuntos jurídicos 50
9.1. Tarifas 51
9.1.1. Tarifas de emissão e renovação de certificados 51
9.1.2. Tarifas de acesso ao certificado 51
9.1.3. Tarifas de revogação ou de acesso à informação de status 51
9.1.4. Tarifas para outros serviços 51
9.1.5. Política de reembolso 51
9.2. Responsabilidade Financeira 51
9.2.1. Cobertura do seguro 51
9.2.2. Outros ativos 51
9.2.3. Cobertura de seguros ou garantia para entidades finais 51
9.3. Confidencialidade da informação do negócio 51
9.3.1. Escopo de informações confidenciais 51
9.3.2. Informações fora do escopo de informações confidenciais 51
9.3.3. Responsabilidade em proteger a informação confidencial 52
9.4. Privacidade da informação pessoal 52
9.4.1. Plano de privacidade 52
9.4.2. Tratamento de informação como privadas 52
9.4.3. Informações não consideradas privadas 52
9.4.4. Responsabilidade para proteger a informação privadas 52
9.4.5. Aviso e consentimento para usar informações privadas 52
9.4.6. Divulgação em processo judicial ou administrativo 53
9.4.7. Outras circunstâncias de divulgação de informação 53
9.4.8. Informações a terceiros 53
9.5. Direitos de Propriedade Intelectual 53

9.6. Declarações e Garantias....53
9.6.1. Declarações e Garantias da AC....53
9.6.2. Declarações e Garantias da AR....54
9.6.3. Declarações e garantias do titular....54
9.6.4. Declarações e garantias das terceiras partes....54
9.6.5. Representações e garantias de outros participantes....54
9.7. Isenção de garantias....54
9.8. Limitações de responsabilidades....54
9.9. Indenizações....54
9.10. Prazo e Rescisão....55
9.10.1. Prazo....55
9.10.2. Término....55
9.10.3. Efeito da rescisão e sobrevivência....55
9.11. Avisos individuais e comunicações com os participantes....55
9.12. Alterações....55
9.12.1. Procedimento para emendas....55
9.12.2. Mecanismo de notificação e períodos....55
9.12.3. Circunstâncias na qual o OID deve ser alterado.....55
9.13. Solução de conflitos....55
9.14. Lei aplicável....55
9.15. Conformidade com a Lei aplicável....55
9.16. Disposições Diversas....55
9.17. Outras provisões....56
10. Documentos referenciados....56
11. Referências Bibliográficas....56

Controle de alterações (a partir da resolução 151/2019)

Resolução que aprovou a alteração	Item alterado	Descrição da alteração	Versão
Resolução CG ICP-Brasil nº 151/2019	Geral	Adequação aos critérios de auditoria contínua e padrões criptográficos da cadeia v5.	8.0
Resolução CG ICP-Brasil nº 175/2020	Capítulo 5 e 6	Atualização dos requisitos operacionais de sala-cofre e parâmetros de criptografia assimétrica.	8.1
Resolução CG ICP-Brasil nº 177/2020	Estrutura Geral	Ajuste à estrutura preliminar do DOC-ICP-05 v6.0 e requisitos de conformidade operacional.	8.2
Resolução CG ICP-Brasil nº 181/2021	Seções 3 e 4	Inserção de regras preliminares para identificação de representantes e emissão de LCR.	8.3
Resolução CG ICP-Brasil nº 188/2022	Capítulo 6 e 7	Atualização de algoritmos de hash (SHA-2) e extensões de certificados no padrão RFC 5280.	8.4
Resolução CG ICP-Brasil nº 197/2023	Capítulo 5	Revisão das políticas de auditoria, perfil de acesso de segurança e plano de desastre.	9.0
Resolução CG ICP-Brasil nº 211/2024	Geral	Revisão do ciclo de vida das chaves criptográficas e processos de credenciamento.	9.1
Resolução CG ICP-Brasil nº 218/2026	Integral	Adequação integral ao DOC-ICP-05 v7.0 (Resolução CG ICP-Brasil nº 177/2020, com redação dada pela Resolução nº 218/2026) e à IN ITI nº 36/2026; reestruturação completa do Capítulo 3 (Identificação e Autenticação); harmonização do rito de identificação das ACs subordinadas pelo rito de credenciamento; exclusão de referências não aplicáveis (CA/Browser Forum, entidades privadas, Juntas	10.0

		Comerciais, CNO); correção de remissões internas.	

1. INTRODUÇÃO

A ICP-Brasil é uma infraestrutura de chaves públicas e confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

1.1. Visão Geral

1.1.1. A Autoridade Certificadora da Justiça (AC-JUS) é uma Autoridade Certificadora de 1º nível integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), subordinada diretamente à Autoridade Certificadora Raiz (AC Raiz - Instituto Nacional de Tecnologia da Informação - ITI) e vinculada administrativamente e tecnicamente ao Conselho da Justiça Federal (CJF). A AC-JUS tem por atribuição exclusiva a emissão, distribuição, renovação e gerenciamento do ciclo de vida de certificados digitais para Autoridades Certificadoras subordinadas de 2º nível, autorizadas pelo Comitê Gestor da AC-JUS a operar de acordo com as normas e procedimentos definidos pela AC-JUS e da ICP-Brasil

1.1.2. Toda DPC elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.1.3. A estrutura desta DPC está baseada na RFC 3647.

1.1.4. A AC-JUS mantém todas as informações desta DPC sempre atualizadas.

1.1.5. Este documento compõe o conjunto normativo da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.

1.2. Nome do documento e identificação

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

1.2.2. A AC-JUS é uma AC de 1º nível que emite certificados digitais somente para outras AC´s , denominadas AC de 2º nível as quais emitem certificados aos usuários finais.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

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

1.3.2. Autoridades de Registro

1.3.2.1. Os processos de identificação, cadastramento e recebimento de solicitações de renovação e revogação das AC de nível imediatamente subsequente ao da AC-JUS, são de competência de sua unidade administrativa, denominada AR-JUS.

a) A AC-JUS disponibiliza e mantém atualizada na página http://www.acjus.jus.br as informações referentes à unidade administrativa, o seu endereço e os meios para contato.
b) Não se aplica.

1.3.3. Titulares de Certificado

Os titulares dos certificados emitidos pela AC-JUS são Autoridades Certificadoras de nível imediatamente subsequente ao seu.

1.3.4. Partes Confiáveis

Considera-se terceira parte a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas no âmbito da ICP-Brasil.

1.3.5. Outros participantes

A relação de ACs e PSS vinculados à AC-JUS está publicada na url https://acjus.jus.br/acjus/ac-e-ar-credenciadas.

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do Certificado

Os certificados definidos por esta DPC AC-JUS são utilizados exclusivamente para a assinatura de certificados digitais de Autoridades Certificadoras de nível imediatamente subsequente ao seu e de sua própria Lista de Certificados Revogados (LCR).

1.4.2. Uso proibitivo do Certificado

Os certificados emitidos pela AC Raiz não podem identificar ou verificar qualquer entidade ou assinatura além dos propósitos descritos nesta DPC

1.5. Política de Administração

1.5.1. Organização administrativa do documento

Nome da AC: Autoridade Certificadora da Justiça – AC-JUS
Nome do órgão responsável: Conselho da Justiça Federal

1.5.2. Contatos

Endereço: SCES Lote 9 – Trecho 3, Polo 8, 2o andar – CJF/STI/ACJUS, CEP 70200-003, Brasília – DF
Telefones: (61) 3022-7407 – 3022-7410 – 3022-7400
Página web: http://www.acjus.jus.br
E-mail: acjus@cjf.jus.br / paulo.martins@cjf.jus.br

1.5.3. Pessoa que determina a adequabilidade da DPC para a política

Responsável: Paulo Martins Inocêncio
E-mail: paulera@cjf.jus.br / acjus@cjf.jus.br
Telefones: (61) 3022-7407

1.5.4. Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.
Os procedimentos de aprovação da DPC da AC-JUS são estabelecidos a critério do CG da ICP-Brasil

1.6. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	*Automatic Certificate Management Environment*
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas

CPF	Cadastro de Pessoas Físicas
CS	*Code Signing*
CSR	*Certificate Signing Request*
DETRAN	Departamento Nacional de Trânsito
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation* (*WebTrust for Certification Authorities*)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF PKIX	*Internet Engineering Task Force - Public-Key Infrastructured (X.509)*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITSEC	*Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union* Lista de Certificados Revogados
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
OM-BR	Objetos Metrológicos ICP-Brasil
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIN	*Personal Identification Number (*Redação dada pela Resolução CG ICP-Brasil n° 204, de 2022)
PIS	Programa de Integração Social
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
PUK	*PIN Unbloking Key (*Redação dada pela Resolução CG ICP-Brasil n° 204, de 2022)
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SIGEPE	Sistema de Gestão de Pessoal da Administração Pública Federal
SNMP	*Simple Network Management Protocol*
SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
TLS	*Transport Layer Security*
TSDM	*Trusted Software Development Methodology*
TSE	Tribunal Superior Eleitoral
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

São disponibilizados no repositório da AC-JUS, logo após sua emissão, os certificados por ela emitidos e sua LCR.

2.1. Repositórios

2.1.1. Obrigações

a) A AC-JUS publica e disponibiliza suas LCR imediatamente após sua emissão e os certificados das AC de nível imediatamente subsequente ao seu, após aprovação e publicação pelo ITI, nas páginas web da AC-JUS em http://www.acjus.jus.br
b) O repositório da AC-JUS está disponível para consulta durante 24(vinte e quatro) horas por dia, 7 (sete) dias por semana.
c) O controle de acesso às informações publicadas pela AC-JUS obedece às normas, critérios, práticas e procedimentos da ICP-Brasil.

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

a) Endereço físico:
   i. Para LCR : SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900. Endereço lógico e url http://lcr.acjus.jus.br/ ;
   ii. Para demais informações SCES Lote 09 Trecho 3 Polo 08 CEP 70.200-003 Brasília -DF e *url* http://www.acjus.jus.br/
b) Disponibilidade: aquela definida no item 2.2.2 desta DPC AC-JUS;
c) Protocolos de acesso: HTTP e HTTPS;
d) Requisitos de segurança:
   i. Os servidores físicos devem estar situados em ambiente de segurança nível 4 conforme definido no item 5.1.2.1.8.;
   ii. A frequência de realização de backup deve ser diária;
   iii. Os procedimentos de manutenção e os perfis técnicos de operação devem ser formalmente definidos;
   iv. Os registros de logs devem ser auditados conforme a frequência definida no item 5.4.2 desta DPC;
   v. Devem ser realizadas análises periódicas de vulnerabilidades;
   vi. A arquitetura segurança para proteção de perímetro deve ser composta por, no mínimo, Firewall, IPS e AntiDDoS;
   vii. A monitoração dos eventos de segurança ou indisponibilidade deve ser realizada por equipe especializada em regime 24x7.

2.1.3. O repositório da AC-JUS está disponível para consulta durante 24(vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.4. A AC-JUS disponibiliza a sua LCR nos endereços:

Versão	Repositório
v5	http://lcr.acjus.jus.br/acjusv5.crl.
v6	http://lcr.acjus.jus.br/acjusv6.crl

2.2. Publicação de informações dos certificados

2.2.1. A AC-JUS publica e disponibiliza suas LCR em “http://lcr.acjus.jus.br” e os certificados das AC de nível imediatamente subsequente ao seu nas páginas web da AC-JUS .

2.2.2. AS informações abaixo, entre outras, são publicadas na página web da AC-JUS em http://www.acjus.jus.br, 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.

a) Seus próprios certificados
b) Suas LCRs
c) Sua DPC
d) Não se aplica
e) Não se aplica
f) uma relação, regularmente atualizada, contendo os PSSs, PSBios e PSCs vinculados

2.3. Tempo ou frequência de publicação

2.3.1. As LCR são publicadas imediatamente após sua emissão pela AC-JUS. As LCR são emitidas e publicadas a cada 90 dias, no máximo, independentemente de haver alteração. Os certificados são publicados no repositório após a aprovação e publicação pela AC Raiz. Esta DPC AC-JUS, é publicada após aprovação pela AC Raiz da ICP-Brasil.

2.4. Controles de acesso aos repositórios

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

Não há qualquer restrição ao acesso para consulta a esta DPC, aos certificados emitidos e às LCR da AC-JUS. São utilizados controles de acesso apropriados para restringir e controlar a escrita nos locais de armazenamento e publicação, o que será permitido 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.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC-JUS verifica a autenticidade da identidade e/ou atributos das entidades da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As entidades estão proibidas de usar nomes em seus certificados que violem os diretos de propriedade intelectual de terceiros. A AC-JUS se reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1. Atribuição de Nomes

3.1.1. Tipos de nomes

3.1.1.1. As AC de nível imediatamente subsequente ao da AC-JUS, titulares de certificados emitidos pela AC-JUS, terão um nome que as identifique univocamente no âmbito da ICP-Brasil. Essa identificação dar-se-á pelo DN (Distinguished Name) – do padrão ITU X.500.

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

3.1.2. Necessidade de nomes serem 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.

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4. Regras para interpretação de vários tipos de nomes

3.1.4.1. Nomes distintos em certificados são interpretados usando os padrões ITU-T X.501 e a sintaxe ASN.1.

3.1.4.2. É vedado o uso de nomes nos certificados que violem os direitos de propriedade intelectual de terceiros

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.

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.

3.2. Validação Inicial de Identidade

Os seguintes requisitos e procedimentos gerais serão seguidos durante o processo de validação inicial de identidade:
São realizados os seguintes processos:

i. identificação e cadastro iniciais do titular do certificado: identificação da pessoa jurídica, titular do certificado, com base nos documentos de identificação citados no item 3.2.2, observado o quanto segue:

   a) Não se aplica;
   b) comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica da AC candidata e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação

ii. emissão do certificado: conferência dos dados da solicitação de certificado com os constante dos documentos apresentados e liberação da emissão do certificado no sistema da AC. A extensão *SubjectAlternativeName* não é utilizada em certificados de autoridade certificadora. A AC candidata deve ter tido sua DPC previamente aprovada pelo ITI.

3.2.1. Método para comprovar o controle de chave privada

A confirmação de que a entidade solicitante controla a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada conforme as referências contidas nas 4210 e 6712, relativos a POP (Proof of Possession). São realizados os seguintes procedimentos:

a) Representantes da AC-JUS acompanharão no ambiente da AC candidata, a geração do par de chaves e da solicitação do certificado (Certificate Request PKCS#10).
b) A solicitação será gravada em mídias, as quais serão verificadas e guardadas em envelopes lacrados.
c) Os envelopes serão então levados ao ambiente off-line da AC-JUS, onde será selecionado um dos envelopes, o qual será verificado quanto à violação e aberto na presença de representantes da AC-JUS, da AC candidata e de testemunhas do PSS da AC-JUS.

d) A mídia será verificada novamente e então utilizada no processo de emissão do certificado da AC subsequente.

3.2.2. Autenticação da Identidade de uma organização

3.2.2.1. A confirmação da identidade de uma AC subordinada é feita com a utilização dos procedimentos de identificação da organização previstos na IN ITI nº 36/2026 onde aplicável. A solicitação de credenciamento ou renovação de certificado de uma AC subordinada à AC -JUS é sempre aprovada previamente pela AC-Raiz. A confirmação da identidade da AC subordinada, pessoa jurídica titular do certificado, é realizada de forma presencial, observando:

I - Relativos à sua habilitação jurídica:

a) se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do CNPJ;
b) se entidade privada:
    i. ato constitutivo ou documento equivalente, devidamente publicado ou registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais;
    ii. documentos da eleição de seus representantes legais, quando aplicável;

II - Relativos à sua habilitação fiscal:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ, com situação cadastral ativa ou
b) prova de inscrição no Cadastro Nacional de Obras – CNO.

Nota: As confirmações dos documentos poderão ser feitas de forma eletrônica em barramentos ou aplicações oficiais. Não é permitida a emissão de certificados digitais para entidades que estejam com a situação do CNPJ como "Baixada" ou "Nula" junto à Secretaria Especial da Receita Federal do Brasil.

3.2.2.2. Será realizada a confirmação da identidade da organização e da pessoa física responsável pelo certificado, bem como a verificação da origem e integridade do Termo de Titularidade. Toda documentação apresentada constará do dossiê eletrônico do titular do certificado.

3.2.3. Autenticação da Identidade de um indivíduo

A confirmação da identidade de um indivíduo que se apresenta como representante de uma AC de nível imediatamente subsequente ao da AC JUS é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

3.2.3.1. Documentos para efeito de identificação de um indivíduo:

As solicitações de certificados, para as AC subordinadas, e a emissão do certificado devem ser acompanhada por pessoa física legalmente habilitada responsável, a qual deverá apresentar presencialmente a seguinte documentação, em sua versão original acompanhada de cópia legível e que permita sua identificação

a) Apresentação da seguinte documentação em sua versão original oficial física ou digital:
    i. Carteira de Identidade Nacional – CIN ou outro Registro de Identidade, se brasileiro;
    ii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
    iii. Passaporte, se estrangeiro não domiciliado no Brasil
    iv. Procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação caso não seja um dos representantes habilitados definidos

no ato constitutivo ou documento equivalente, devidamente publicado ou registrado no órgão competente;

b) Consultar a inscrição no cadastro de Pessoa Física CPF;

c) Não se aplica;

d) Não se aplica;

3.2.3.2. A identificação será realizada nas seguintes modalidades:

a) Comparecimento presencial;

b) uso de certificado ICP-Brasil válido;

c) Não se aplica; e

d) Não se aplica.

3.2.3.3. Não se aplica;

3.2.3.4. Não se aplica;

3.2.4. Informações não verificadas do titular do certificado

Não se aplica

3.2.5. Validação das Autoridades

Na emissão de certificado de AC subsequente é verificado se a pessoa física é o representante legal ou procurador da AC.

3.2.6. Critérios para interoperabilidade

Não se aplica

3.2.7. Autenticação da identidade de equipamento ou aplicação

Não se aplica

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. O processo de geração pela AC-JUS de um novo certificado para uma AC de nível imediatamente subsequente ao seu pode ser feito de forma simplificada, antes da expiração da validade do certificado vigente da AC.

Para isso, um representante legal da AC deve formalizar a solicitação por ofício e preencher e assinar em papel ou digitalmente, FORMULÁRIO DE REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO[8]. Após o recebimento desse formulário, desde que a documentação esteja regularmente atualizada, a AC-JUS iniciará o processo de emissão do novo certificado.

3.3.2. Aplicam-se os mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3

3.3.3. Para casos específicos de expiração ou revogação de um certificado de AC de nível imediatamente subsequente ao da AC-JUS , aquela AC deverá executar os processos regulares de geração so seu novo par de chaves

3.4. Identificação e Autenticação para solicitação de revogação

3.4.1. O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.9.2 podem solicitar a revogação do certificado de uma AC de nível imediatamente subsequente ao da AC-JUS

3.4.2. O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3. Solicitações de revogação de certificados devem ser registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. Solicitação de Certificado

A AC-JUS somente aceitará solicitações de certificado para ACs subsequentes que já tenham sido auditadas pela AC-Raiz e estejam em pleno funcionamento e operando em outras cadeias da ICP-Brasil.

Além da aprovação pelo Comitê Gestor da AC-JUS, os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado são:

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
b) Não se aplica;
c) um termo de acordo assinado pelos representantes legais da AC e da AC-JUS.
d) não se aplica
e) não se aplica

Nota : o termo de acordo poderá ser assinado digitalmente com certificado digital pelos representantes legais da AC-JUS e da AC candidata.

4.1.1. Quem pode submeter uma solicitação

4.1.1.1. 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 Comitê Gestor da AC-JUS para aprovação. A solicitação de certificado para AC de nível imediatamente subsequente ao da AC responsável somente será 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 ENTIDADESINTEGRANTES DA ICP-BRASIL [4].

4.1.1.2. Não se aplica

4.1.1.3. A AC subsequente deverá encaminhar a solicitação de certificado à AC emitente por meio de seus representantes legais, utilizando o padrão definido regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

4.1.1.4. A solicitação de um certificado para a AC-JUS é feita por seus representantes legais á AC-RAIZ.

4.1.2. Processo de registro e responsabilidades

4.1.2.1. Responsabilidades da AC

4.1.2.1.1. A AC-JUS é responsável pelos danos a que der causa

4.1.2.1.2. A AC responde solidariamente pelos atos das entidades de sua cadeia de certificação: AC subordinadas, AR e PSS

4.1.2.1.3. Não se aplica.

4.1.2.2. Obrigações da AC-JUS

a) operar de acordo com esta DPC;
b) a geração e gerenciamento dos 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 de AC de nível imediatamente subsequente ao seu;
h) informar a emissão do certificado ao respectivo solicitante;
i) a revogação dos certificados por ela emitidos;
j) emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR);
k) publicar esta DPC, aprovada e implementada no endereço: http://www.acjus.jus.br/acjus/dpcacjus.pdf
l) publicar em sua página web as informações definidas no item 2.2.2 deste documento;
m) não se aplica;
n) não se aplica;
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 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 a manutenção de contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil; não se aplica;
u) não se aplica;
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;
x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada às ACs que utilizam de seus serviços; e
y) não se aplica;

4.1.2.3. não se aplica

4.1.2.4. não se aplica

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

A AC executa as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2. Aprovação ou rejeição de pedidos de certificado

4.2.2.1. A AC pode aceitar ou rejeitar pedidos de certificados das AC imediatamente subsequente de acordo com os procedimentos descritos no item 4.1 desta DPC.

4.2.2.2. A AC pode, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

4.2.3. Tempo para processar a solicitação de certificado

A AC-JUS cumpre os procedimentos determinados na ICP-Brasil. Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

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

A emissão dos certificados das AC de nível imediatamente subsequente à AC-JUS é feita em equipamentos que operam off-line. A AC-JUS entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC habilitada.

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

4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado

O certificado de AC subsequente é entregue aos seus representantes legais, que acompanham a cerimonia de emissão, imediatamente após emitido.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.1.1. 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.

4.4.1.2. A aceitação do certificado se dá após a verificação pela AC e assinatura do termo de acordo ou na primeira utilização da chave privada correspondente. 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 definidas pela AC-JUS para emissão de certificados na sua cadeia de certificação.

4.4.1.3. A AC de nível imediatamente subsequente atestará através de seus representantes legais, mediante assinatura do “Termo de Acordo”, o recebimento do certificado emitido.

4.4.2. Publicação do certificado pela AC

O certificado da AC-JUS e os certificados das ACs de nível imediatamente subsequente ao seu são publicados de acordo com item 2.2 desta DPC.

4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades

A notificação de emissão de certificado pela AC Raiz se dará de acordo com item 2.2 da DPC da AC RAIZ.

4.5. Usabilidade do par de chaves e do certificado

A AC de nível imediatamente subsequente à AC-JUS deve operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementar, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[5].

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.1.1. A AC titular deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto na sua própria DPC.

4.5.1.2. Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos pela AC responsável pela DPC, constantes dos termos acordo de que trata o item 4.1, incluem, os itens abaixo relacionados:

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 , códigos de ativação e dispositivos criptográficos;
c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
d) conhecer os seus direitos e obrigações, contemplados pela DPC e outros documentos aplicáveis da ICP-Brasil;
e) informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente; e
f) não se aplica

4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Não se aplica.

4.6.1. Circunstâncias para renovação de certificados

Não se aplica.

4.6.2. Quem pode solicitar a renovação

Não se aplica

4.6.3. Processamento de requisição para renovação de certificados

Não se aplica

4.6.4. Notificação para nova emissão de certificado para o titular

Não se aplica.

4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

Não se aplica.

4.6.6. Publicação de uma renovação de um certificado pela AC

Não se aplica.

4.6.7. Notificação de emissão de certificado pela AC para outras entidades

Em acordo com item 4.3 desta DPC.

4.7. Nova chave de certificado (Re-key)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica

4.7.2. Quem pode requisitar a certificação de uma nova chave pública

Não se aplica

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica

4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica

4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades

Não se aplica

4.8. Modificação de certificado

Não se aplica

4.8.1. Circunstâncias para modificação de certificado

Não se aplica

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica

4.8.6. Publicação de uma modificação de certificado pela AC

Não se aplica

4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades

Não se aplica

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

4.9.1.1. 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.

4.9.1.2. 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 ou da sua mídia armazenadora; ou
e) por decisão judicial.

4.9.1.3. Observa-se ainda que:

a) A AC-JUS deverá revogar, no prazo definido no item 4.9.3.3, 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.

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

4.9.1.5. A autenticidade da LCR deverá também ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

4.9.2. 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 titular do certificado;
b) não se aplica;
c) não se aplica;
d) pela AC-JUS;
e) não se aplica;
f) por determinação do CG da ICP-Brasil ou da AC Raiz;
g) não se aplica;
h) não se aplica;
i) não se aplica;
j) não se aplica;
k) por decisão judicial.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. A solicitação de revogação de certificado de AC subsequente deve ser feita através do formulário SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC [9]. Esse formulário deverá ser assinado pelo representante legal da AC. Se utilizada versão digital do documento, este deverá estar assinado digitalmente. O documento deverá ser entregue à unidade administrativa da AC-JUS pelo representante legal da AC subsequente, e, em se tratando de formulário em papel, será assinado no ato da entrega.

4.9.3.2. 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 serão documentadas; e

d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.9.3.3. O prazo máximo para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificados previstos pela ICP-Brasil é de 24 (vinte e quatro) horas.

4.9.3.4. O prazo máximo para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação é de 24 (vinte e quatro) horas.

4.9.3.5. 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.

4.9.3.6. Não se aplica.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1.

4.9.4.2. não se aplica

4.9.5. Tempo em que a AC deve processar o pedido de revogação

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC deve processar a revogação imediatamente após a análise do pedido.

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

Antes de confiar em um certificado, a parte confiável deve confirmar a validade de cada certificado na cadeia de certificação de acordo com os padrões IETF PKIX, incluindo a verificação da validade do certificado, encadeamento do nome do emissor e titular, restrições de uso de chaves e de políticas de certificação e o status de revogação por meio de LCRs ou respostas OCSP identificados em cada certificado na cadeia de certificação.

4.9.7. Frequência de emissão de LCR

4.9.7.1. A frequência definida para a emissão de LCR referente a certificados de AC de nível imediatamente subsequente ao da AC-JUS é de, no máximo, 90 dias.

4.9.7.2. Não se aplica.

4.9.7.3. A frequência máxima para emissão de LCR referente a certificado de AC, é de 90 dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente à AC-JUS, será emitida nova LCR no prazo previsto no item 4.9.3.4 , serão notificadas todas as AC de nível imediatamente subsequente ao seu e a AC-Raiz.

4.9.7.4. Não se aplica.

4.9.8. Latência máxima para a LCR

A LCR é divulgada no repositório em no máximo 4 (quatro) horas após sua geração.

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

Não se aplica

4.9.10. Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11. Outras formas disponíveis para divulgação de revogação

4.9.11.1. Informações de revogação de certificados de AC de nível imediatamente subsequente ao da AC-JUS poderão ser publicadas nas páginas WEB da AC-JUS https://www.acjus.jus.br

4.9.11.2. Não se aplica

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. No caso do comprometimento da chave privada de uma AC de nível imediatamente subsequente ao da AC-JUS, a mesma deverá notificar o fato imediatamente à AC-JUS.

4.9.12.2. A comunicação do comprometimento ou suspeita de comprometimento da chave privada de uma AC poderá ser feita, por correio eletrônico em documento assinado digitalmente pelo representante legal da AC.

4.9.13. Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, salvo em casos específicos e determinados pelo Comitê Gestor .

4.9.14. Quem pode solicitar suspensão

A AC, aprovados pelo Comitê Gestor

4.9.15. Procedimento para solicitação de suspensão

Não se aplica

4.9.16. Limites no período de suspensão

Não se aplica

4.10. Serviços de status de certificado

4.10.1. Características operacionais

A AC fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR

4.10.2. Disponibilidade dos serviços

Ver item 4.9

4.10.3. Funcionalidades operacionais

Ver item 4.9

4.11. Encerramento de atividades

4.11.1. A AC-JUS observa os procedimentos descritos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [4] nos casos de extinção ou encerramento dos serviços da AC responsável, de uma AR, PSS ou PSBios a ela vinculados.

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

a) notificar a AC Raiz da ICP-Brasil;
b) notificar todas as entidades subordinadas;
c) providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;
d) a transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-JUS 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

4.12. Custódia e recuperação de chave

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas, de AC .

4.12.1. Política e práticas de custódia e recuperação de chave

Não se aplica

4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

Não se aplica

5. Controles Operacionais , Gerenciamento e de Instalações

5.1. Controle Físico

5.1.1. Construção e localização das instalações de AC

5.1.1.1. A operação da AC-JUS é executada dentro de um ambiente físico seguro em área de instalação altamente protegida. A localização e o sistema de certificação utilizado para a operação da AC-JUS não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Todas as instalações do PSS da AC- JUS, relevantes para os controles de segurança física, foram feitas 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;
c) e sistema de aterramento e de proteção contra descargas atmosféricas; e
d) iluminação de emergência.

5.1.2. Acesso físico nas instalações de AC

O acesso físico às dependências do PSS AC-JUS é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [6]. 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.

5.1.2.1. Níveis de Acesso

5.1.2.1.1. 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.

5.1.2.1.2. O primeiro nível – ou nível 1– Situa-se após a primeira barreira de acesso às instalações do PSS 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.

5.1.2.1.3. 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, pagers, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. 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.

5.1.2.1.5. 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.

5.1.2.1.6. 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.

5.1.2.1.7. 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.

5.1.2.1.8. 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.

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

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

5.1.2.1.11. São três os tipos de serviço abrigados pela sala cofre no quarto nível:

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

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

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

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

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

5.1.2.2. Sistema físico de detecção

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

5.1.2.2.2. As mídias de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

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

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

5.1.2.2.5. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

5.1.2.2.6. 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.

5.1.2.3. Sistema de Controle de Acesso

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

5.1.2.4. Mecanismos de emergência

5.1.2.4.1. 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.

5.1.2.4.2. 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.

5.1.3. Energia e ar condicionado nas instalações de AC

5.1.3.1. 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;

5.1.3.2. Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados;

5.1.3.3. 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;

5.1.3.4. 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.

5.1.3.5. 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[6]. Qualquer modificação nessa rede é previamente documentada.

5.1.3.6. Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

5.1.3.7. 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 a falhas.

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9. O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10. 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.

5.1.4. Exposição à água nas instalações de AC

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

5.1.5. Prevenção e proteção contra incêndio nas instalações de AC

5.1.5.1. Todas as instalações do PSS da AC-JUS possuem sistemas de prevenção contra incêndio. Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2. Nas instalações do PSS da AC-JUS não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. A sala cofre possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala cofre são eclusas, uma porta só se abre quando a anterior está fechada.

5.1.5.4. Em caso de incêndio nas instalações do PSS da AC-JUS, a temperatura interna da sala cofre não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.6. Armazenamento de mídia nas instalações de AC

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

5.1.7. Destruição de lixo nas instalações de AC

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo;

5.1.7.2. Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos;

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

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

5.2. Controles Procedimentais

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

5.2.1. Perfis qualificados

5.2.1.1. A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2. A AC-JUS estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as ações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

5.2.1.3. Todos os operadores do sistema de certificação da AC-JUS recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.3.1. Não se aplica

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) do PSS da AC-JUS.

5.2.3. Identificação e autenticação para cada perfil

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

a) Ser incluído em uma lista de acesso às instalações do PSS da AC-JUS;
b) ser incluído em uma lista para acesso físico ao sistema de certificação do PSS da AC-JUS;
c) receber um certificado para executar suas atividades operacionais do PSS da AC-JUS;
d) receber uma conta no sistema de certificação do PSS da AC-JUS.

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

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

5.2.3.3. O PSS da 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.

5.2.4. Funções que requerem separação de deveres

A AC realiza a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

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[6].

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 poderá ser pedido o histórico de processos administrativos.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC-JUS, 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;
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 3.2.2, 3.2.3 e 3.2.7; 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 envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC-JUS. Treinamentos de reciclagem são realizados pela AC-JUS sempre que necessário.

5.3.5. Frequência e sequência de rodízios de cargos

A AC-JUS não implementa rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC-JUS suspenderá o seu acesso ao sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima conterá, no mínimo, os seguintes itens:

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

5.3.6.3. Concluído o processo administrativo, a AC-JUS encaminhará suas conclusões à AC Raiz.

5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

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

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC-JUS e do PSS, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, será contratado conforme o estabelecido nas POLÍTICA DE SEGURANÇA DA ICP-BRASIL[6] e na Política de Segurança da AC-JUS.

5.3.8. Documentação fornecida ao pessoal

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

a) esta DPC;
b) não se aplica;
c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[6];
d) documentação operacional relativa às suas atividades; e
e) 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.

5.4. Procedimentos de Auditoria de Segurança

5.4.1. Tipos de Evento Registrados

5.4.1.1. 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 (logoff);
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.

5.4.1.2. 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.

5.4.1.3. 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.

5.4.1.4. 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.

5.4.1.5. 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[6].

5.4.1.6. Não se aplica.

5.4.1.7. Não se aplica.

5.4.2. Frequência de auditoria de registros (logs)

5.4.2.1. 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.

5.4.2.2. 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.

5.4.3. 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 5.5.

5.4.4. Proteção de registro (log) de Auditoria

5.4.4.1. 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.

5.4.4.2. 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.

5.4.4.3. 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.

5.4.5. 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.

5.4.6. Sistema de coleta de dados de auditoria

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

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de log-in e log-out	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
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 Backup e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de software e hardware	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

5.4.7. 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.

5.4.8. 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.

5.5. Arquivamento de Registros

5.5.1. 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 5.4.1;
h) correspondências formais;

5.5.2. 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) os dossiês dos titulares, de solicitação e da revogação de certificados e os termos de acordo, titularidade e responsabilidade serão retidos por, no mínimo 7 (sete) anos a contar da data de expiração ou revogação do certificado. Prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado; e
c) as demais informações, inclusive registros de auditoria são retidas por, no mínimo, 7 (sete) anos.

5.5.3. 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[6]

5.5.4. Procedimentos para cópia de arquivos

5.5.4.1. A primeira cópia é armazenada em servidor de rede apropriado em ambiente nível 4. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo da AC , no site de backup e recebem o mesmo tipo de proteção utilizada por ela no arquivo principal

5.5.4.2. As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.

5.5.4.3. A AC-JUS garante que a verificação da integridade dessas cópias de segurança, é realizada no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para datação de registros

Os servidores da AC são sincronizados com a hora GMT fornecida pela AC RAIZ por meio de sua Fonte Confiável do Tempo – FCT. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.
No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

5.5.6. 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

5.5.7. Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC-JUS é verificada:
a) Na ocasião em que o arquivo é preparado;
b) Semestralmente no momento de uma auditoria de segurança programada;
c) Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

5.6. Troca de chave

5.6.1. 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.

5.6.2. Não se aplica.

5.7. Comprometimento e Recuperação de Desastre

5.7.1. Procedimentos gerenciamento de incidente e comprometimento

5.7.1.1. Os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres estão descritos no Plano de Continuidade de Negócio – PCN do PSS da AC-JUS, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [6], para garantir a continuidade dos seus serviços críticos.

5.7.1.2. Não se aplica

5.7.2. Recursos computacionais, software ou dados corrompidos

A AC-JUS possui um 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.

5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1. Certificado de entidade revogado

A AC possui um Plano de Continuidade de Negócio – PCN, 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.
c) É gerado novo par de chaves da AC-JUS e solicita-se novo certificado à AC RAIZ
d) Iniciam-se os procedimentos para emissão de novos certificados digitais para as AC de nível imediatamente subsequente

5.7.3.2. Chave de entidade comprometida

O PSS da 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

5.7.4. Capacidade de continuidade de negócio após desastre

O PSS da 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.

5.8. Extinção dos serviços de AC-JUS ou PSS

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

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

a) notificar a AC Raiz da ICP-Brasil;
b) notificar todas as entidades subordinadas;
c) providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;
d) a transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-JUS 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.

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 que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7], padrão "Homologação da ICP-Brasil NSH-3", 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.

6.1.1.3. Não se aplica.

6.1.1.4. O processo de geração do par de chaves da AC-JUS é realizado em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7], padrão "Homologação da ICP-Brasil NSH-3"

6.1.1.5. Não se aplica.

6.1.1.6. O par de chaves da AC-JUS é gerado em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA 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. Entrega da chave pública da AC às terceiras partes

6.1.4.1. 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[7];
b) Diretório;
c) Páginas web da AC-JUS (http://www.acjus.jus.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 será de 4096 (quatro mil e noventa e seis) bits observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7].

6.1.6. Geração de parâmetros de chaves assimétricas

6.1.6.1. Os parâmetros de geração de chaves assimétricas da AC-JUS seguem o padrão Homologação da ICP-Brasil NSH-3., definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7].

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7].

6.1.7. Propósitos de uso de chave (conforme campo “Key usage” na X.509 v3)

6.1.7.1. As chaves criptográficas das ACs subsequentes à AC-JUS poderão ser utilizadas apenas para assinatura dos certificados por elas emitidos e de suas LCR.

6.1.7.2. A chave privada da AC-JUS é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

As chaves privadas da AC-JUS são geradas, armazenadas e utilizadas apenas em hardware criptográfico com padrão de segurança “Homologação da ICP-Brasil NSH-3”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7], não havendo, portanto, tráfego das mesmas em nenhum momento.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. Toda a geração e armazenamento da chave da AC-JUS e também operações de assinatura de certificados pela AC-JUS, são realizadas em um módulo de hardware criptográfico com padrão de segurança “Homologação da ICP-Brasil NSH-3” de acordo com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7].

6.2.1.2. Os módulos criptográficos das AC subsequentes à AC-JUS devem adotar padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7].

6.2.2. Controle “n de m’ para chave privada

6.2.2.1. A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC-JUS é dividida em “9” partes e distribuídas por “9” custodiantes designados pela AC-JUS (m).

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

6.2.3. Recuperação (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas, de AC.

6.2.4. Cópia de segurança de chave privada

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

6.2.4.2. A AC-JUS mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.

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

6.2.4.4. A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7].

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas da AC não são arquivadas pela AC-JUS.

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

6.2.6. Inserção de chave privada em módulo criptográfico

A chave privada da AC é inserida no módulo criptográfico de acordo com os procedimentos especificados pelo fornecedor do módulo.

6.2.7. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação das chaves privadas da AC-JUS é implementada por meio de cartões criptográficos, protegidos por senha, após a identificação de "2" dos "9" custodiantes da chave criptográfica de ativação. Os custodiantes da chave de ativação serão magistrados ou servidores do Poder Judiciário indicados pelos órgãos representados no Comitê Gestor da AC-JUS.

6.2.9. 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. Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de "2" de "9" dos custodiantes da chave criptográfica de ativação.

6.2.10. 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 serão destruídas. Os agentes autorizados para realizar estas operações são os administradores do sistema e os custodiantes das chaves de ativação da AC-JUS.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da própria AC-JUS e das ACs de nível imediatamente subsequente ao seu 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.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. A chave privada da AC-JUS bem como as chaves privadas das ACs de nível imediatamente subsequente, 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.

6.3.2.2. Não se aplica.

6.3.2.3. A validade admitida para certificados das AC imediatamente subsequentes à AC-JUS é limitada à validade do certificado da AC-JUS, que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC-JUS.

6.4. Dados de ativação

6.4.1. Geração e instalação dos dados de ativação

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

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação.

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

6.4.2.2. Não se aplica.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A AC-JUS garante que a geração de seu par de chaves é realizada em ambiente off-line, para impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos gerais de segurança computacional dos equipamentos utilizados para a geração dos pares de chaves criptográficas das AC titulares de certificados emitidos pela AC-JUS são:

a) Utilização de antivírus, *antitrojan* e *antispyware* instalados, atualizados e habilitados;

b) Utilização de firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades; e

c) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc).

6.5.1.3. Os computadores servidores, utilizados pela AC-JUS, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) Controle de acesso aos serviços e perfis da AC-JUS;

b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC-JUS;

c) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

d) Geração e armazenamento de registros de auditoria da AC-JUS;

e) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e

f) Mecanismos para cópias de segurança (backup).

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

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC-JUS, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC-JUS ou AC subsequente. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC-JUS é preparado e configurado como previsto na política de segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

Não se aplica.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.

6.5.3.2. Não se aplica.

6.5.3.3. Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1. A AC-JUS adota sistema de certificação SGC YWYRA desenvolvido para o Instituto Nacional de Tecnologia da Informação – ITI e licenciado para a AC-JUS por prazo indeterminado. Esse sistema é homologado pelo ITI e está em conformidade com os padrões e normas da ICP-Brasil. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluído os testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do PSS avalia e decide quando será a implementação no ambiente de produção.

6.6.1.2. 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.

6.6.2. Controle de gerenciamento de segurança

6.6.2.1. 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.

6.6.2.2. 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.

6.6.3. Classificação de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Antes de publicadas todas as LCR geradas pela AC são checadas quanto à consistência de seu conteúdo, comparando-a com o conteúdo esperado em relação ao número da LCR, data/hora de emissão e outras informações relevantes.

6.7. Controles de Segurança de Rede

Os computadores servidores da AC-JUS que hospedam os sistemas de certificação operam off-line, fisicamente desconectados de qualquer rede. Os servidores que hospedam o repositório e os sistemas de publicação da AC-JUS adotam os controles que seguem:

6.7.1. Diretrizes Gerais

6.7.1.1. Os controles implementados para garantir a confidencialidade, integridade e disponibilidade dos serviços da AC são os seguintes:

a) Infraestrutura de conectividade, incluindo:
    i. Alojamento seguro de equipamento de comunicação;
    ii. Firewall seguro e serviços de roteador;
    iii. Serviço de LAN seguro; e
    iv. Serviço de internet seguro e redundante;
b) Prevenção incidente e avaliação, incluindo:
    i. Descoberta de intrusão;
    ii. Análise de vulnerabilidade;
    iii. Configuração segura de servidor; e
    iv. Auditorias técnicas.
c) Administração de infraestrutura, incluindo:
    i. Monitoramento de servidor;
    ii. Monitoramento de rede;
    iii. Monitoramento de URL; e
    iv. Relatórios de largura da banda. A

6.7.1.2. Somente os serviços estritamente necessários para o funcionamento do sistema de certificação da AC-JUS estão habilitados.

6.7.1.3. 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 repositório e sistemas de publicação da AC, estão localizados e operam em ambiente de nível 4.

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

6.7.1.5. O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2. Firewall

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

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

6.7.3. Sistema de detecção de intrusão

6.7.3.1. O sistema de detecção de intrusão pode ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao firewall ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do firewall.

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

6.7.3.3. O sistema de detecção de intrusão provê o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4. Registro de acessos não autorizados à rede

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

6.8. Carimbo de Tempo

Não se aplica.

7. Perfis de Certificado e LCR

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC-JUS estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8 de acordo com o perfil estabelecido na RFC 5280.

7.1.1. 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 5280.

7.1.2. Extensões de certificados

Os certificados emitidos pela AC-JUS, sob esta DPC, obedecem às resoluções da ICP-Brasil, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I do DOC-ICP-04, aprovado pela Resolução CG ICP-Brasil nº179, de 20 de outubro de 2020, 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 e keyCertSign e cRLSign são ativados;
d) "Certificate Policies", não crítica:
    i. o campo policyIdentifier contém o OID da PC que a AC titular do certificado implementa;
    ii. o campo policyQualifiers contém o endereço URL da página web onde se obtém a DPC da AC-JUS: http://www.acjus.jus.br/acjus/dpcacjus.pdf
e) o campo "Basic Constraints", crítica: contém o campo cA=*True*;
f) "CRL Distribution Points", não crítica: contém os endereços URL das páginas web onde se obtém as LCR da AC-JUS correspondente ao certificado:

AC-JUS v5	http://lcr.acjus.jus.br/acjusv5.crl

AC-JUS v6	http://lcr.acjus.jus.br/acjusv6.crl

7.1.3. Identificadores de algoritmos

Os certificados emitidos pela AC-JUS v6 e AC-JUS v5, sob as cadeias v12 e v5 da AC RAIZ da ICP-Brasil respectivamente, são assinados com o uso da suite de assinatura sha512WithRSAEncryption (OID=1.2.840.113549.1.1.13), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[7].

7.1.4. Formatos de nome

Para os certificados emitidos sob esta DPC AC-JUS, o nome da AC titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

De 2016 a 2018:

C=BR
O= ICP-Brasil
OU= Autoridade Certificadora da Justiça – AC-JUS
OU = <SMIME, SSL ou Codesigning, de acordo com o tipo de uso escolhido conforme a IN 12/2016 do ITI>
CN= nome da AC titular
(O CN deverá estar na forma "AC <nome da AC titular>-JUS <sigla do tipo de uso> <identificador de versão da cadeia>")

Após 2018

C=BR
O= ICP-Brasil
OU= Autoridade Certificadora da Justiça – AC-JUS
CN= nome da AC titular
(O CN deverá estar na forma "AC <nome da AC titular>-JUS <identificador de versão da cadeia>")

7.1.5. Restrições de nome

Aplicam-se as restrições gerais estabelecidas pela ICP-Brasil, aplicáveis para os nomes de AC titulares de certificados, conforme o documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [5].

a) não serão utilizados sinais de acentuação, tremas ou cedilhas;
b) além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caracter e Código	**NBR9611 (hexadecimal)**
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27

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

7.1.6. OID (Object Identifier) de DPC

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

7.1.7. Uso da extensão "Policy Constraints"

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

7.1.8. Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web (URL) da DPC da AC-JUS: http://www.acjus.jus.br/acjus/dpcacjus.pdf

7.1.9. Semântica de processamento para extensões criticas

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

7.2. Perfil de LCR

7.2.1. Número (s) de versão

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

7.2.2. Extensões de LCR e de suas entradas

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

Campo	Valor	Presença	Criticalidade
5. Extensões X.509v3			
5.1. *Authority Key Identifier*	Hash 160 bits SHA-1 da chave pública da AC que assina a LCR	O	não-crítica
5.2. *CRL Number*	Número sequencial para cada LCR emitida pela AC	O	não-crítica

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

A AC-JUS não implementa serviço de respostas OCSP.

7.3.2. Extensões de OCSP

Não se aplica.

8. Auditoria de conformidade de outras avaliações

8.1. Frequência e circunstâncias das avaliações

As entidades integrantes da ICP-Brasil sofrem auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento

8.2. Identificação/Qualificação do avaliador

8.2.1. 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 ICP-BRASIL [1].

8.2.2. 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 ICP-BRASIL [2].

8.3. Relação do avaliador com a entidade avaliada

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 ICP-BRASIL [2].

8.4. Tópicos cobertos pela avaliação

8.4.1. 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 e com os princípios e critérios definidos pelo *WebTrust.*

8.4.2. A AC-JUS recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e 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 ICP-BRASIL [2].

8.4.3. As entidades da ICP-Brasil diretamente vinculadas à AC-JUS – 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.

8.5. Ações tomadas como resultado de uma deficiência

Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[1] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2].

8.6. Comunicação dos resultados

Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[1] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2].

9. Outros Negócios e assuntos jurídicos

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

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

9.1.2. Tarifas de acesso ao certificado

Não se aplica.

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

Não se aplica.

9.1.4. Tarifas para outros serviços

Não há tarifas previstas pela AC-JUS outros serviços.

9.1.5. Política de reembolso

Não se aplica.

9.2. Responsabilidade Financeira

A responsabilidade da AC será verificada conforme previsto na legislação brasileira.

9.2.1. Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2. Outros ativos

Conforme item 4 desta DPC.

9.2.3. Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3. Confidencialidade da informação do negócio

9.3.1. Escopo de informações confidenciais

9.3.1.1. Todas as informações coletadas que contenham dados pessoais, geradas, transmitidas e mantidas pela AC-JUS são consideradas sigilosas, exceto aquelas informações citadas no item 9.3.2.

9.3.1.2. Como princípio geral, nenhum documento, informação ou registro fornecido à AC-JUS deverá ser divulgado.

9.3.2. Informações fora do escopo de informações confidenciais

Os seguintes documentos da AC são considerados documentos não confidenciais:

a) Certificados e LCR emitidas pela AC;
b) informações corporativas ou pessoais que necessariamente façam parte de certificados ou de diretórios públicos
c) Não se aplica;
d) a DPC da AC-JUS
e) versões públicas de Política de Segurança; e
f) a conclusão dos relatórios de auditoria;

9.3.2.1. Certificados, LCR/OCSP, e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não confidenciais

9.3.2.2. Os seguintes documentos da AC também são considerados documentos não confidenciais:

a) Não se aplica;
b) Qualquer DPC;
c) Versões públicas de Política de Segurança; e
d) Conclusão dos relatórios de auditoria.

9.3.2.3. A AC também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-Brasil

9.3.3. Responsabilidade em proteger a informação confidencial

9.3.3.1. Os participantes que receberem ou tiverem acesso a informações confidenciais devem possuir mecanismos para assegurar a proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

9.3.3.2. As chaves privadas de assinatura digital da AC-JUS foram geradas e são mantidas 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.

9.3.3.3. Os representantes legais das ACs de nível imediatamente subsequente ao da AC-JUS terão a responsabilidade sobre a geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, são responsáveis pela divulgação ou utilização indevida dessas mesmas chaves.

9.3.3.4. Não se aplica.

9.4. Privacidade da informação pessoal

9.4.1. Plano de privacidade

A AC-JUS assegura a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2. Tratamento de informação como privadas

Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC será considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

9.4.3. Informações não consideradas privadas

Informações sobre revogação de certificados de usuários finais e de AC de nível imediatamente subsequente ao da AC são fornecidas na LCR da AC.

9.4.4. Responsabilidade para proteger a informação privadas

A AC-JUS é responsável pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5. Aviso e consentimento para usar informações privadas

As informações privadas obtidas pela AC poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável. 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.
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.

9.4.6. Divulgação em processo judicial ou administrativo

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC será fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.
As informações privadas ou confidenciais sob a guarda da AC poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7. Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8. Informações a terceiros

Como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AC-JUS deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.5. Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

A AC declara e garante o quanto segue:

9.6.1.1. Autorização para certificado

A AC implementa procedimentos para verificar a autorização da emissão de um certificado ICP- Brasil, contidas nos itens 3 e 4 desta DPC. A AC, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das ACs subsequentes e AR na forma de suas DPCs, PCs e normas complementares.

9.6.1.2. Precisão da informação

A AC implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC Raiz, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequentes e AR na forma de suas DPCs, PCs e normas complementares.

9.6.1.3. Identificação do requerente

A AC implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequentes e AR na forma e suas DPCs, PCs e normas complementares.

9.6.1.4. Consentimento dos titulares

A AC implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5. Serviço

A AC mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios, das ACs subsequentes e LCRs.

9.6.1.6. Revogação

A AC revogará certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos Princípios e Critérios WebTrust.

9.6.1.7. Existência Legal

Esta DPC está em conformidade legal com a MP 2.200-2, de 24 de agosto de 2001, e legislação aplicável.

9.6.2. Declarações e Garantias da AR

Em acordo com item 4 desta DPC.

9.6.3. Declarações e garantias do titular

9.6.3.1. 9.6.3.1 Toda informação necessária para a identificação do titular de certificado deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pela AC, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2. 9.6.3.2 A AC deve informar à AC Raiz qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

9.6.4. Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
b) verificar, a qualquer tempo, a validade do certificado.

9.6.4.2. O certificado da AC ou um certificado de AC de nível imediatamente subsequente ao da AC é considerado válido quando:

i. tiver sido emitido pela AC;
ii. não constar como revogado pela AC;
iii. não estiver expirado; e
iv. puder ser verificado com o uso do certificado válido da AC.

9.6.4.3. A utilização ou aceitação de certificados sem a observância das providências descritas é de conta e risco da terceira parte que usar ou aceitar a utilização do respectivo certificado.

9.6.5. Representações e garantias de outros participantes

Não se aplica.

9.7. Isenção de garantias

Não se aplica.

9.8. Limitações de responsabilidades

A AC não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

9.9. Indenizações

A AC responde pelos danos que der causa, e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

9.10. Prazo e Rescisão

9.10.1. Prazo

Esta DPC entra em vigor a partir da publicação que a aprovar, e permanecerá válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.2. Término

Esta DPC vigorará por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.3. Efeito da rescisão e sobrevivência

Os atos praticados na vigência desta DPC são válidos e eficazes para todos os fins de direito, produzindo efeitos mesmo após a sua revogação ou substituição.

9.11. Avisos individuais e comunicações com os participantes

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente ou publicação no Diário Oficial da União.

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC deverá ser submetida para AC Raiz.

9.12.2. Mecanismo de notificação e períodos

Mudança nesta DPC será publicado no site da AC.

9.12.3. Circunstâncias na qual o OID deve ser alterado.

Não se aplica.

9.13. Solução de conflitos

9.13.1. Os litígios decorrentes desta DPC serão solucionados de acordo com a legislação vigente.

9.13.2. Esta DPC não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14. Lei aplicável

Esta DPC é regida pela legislação da República Federativa do Brasil, notadamente a Medida Provisória Nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

9.15. Conformidade com a Lei aplicável

A AC está sujeita à legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em lei.

9.16. Disposições Diversas

9.16.1. Acordo completo

Esta DPC representa as obrigações e deveres aplicáveis à AC-JUS. Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2. Cessão

Os direitos e obrigações previstos nesta DPC são de ordem pública e indisponíveis, não podendo ser cedidos ou transferidos a terceiros.

9.16.3. Independência de disposições

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPC não prejudicará as demais disposições, as quais permanecerão plenamente válidas e eficazes. Neste caso a disposição inválida, nula ou ineficaz será considerada como não escrita, de forma que esta DPC será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.

9.16.4. Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

10. Documentos referenciados

10.1. Os documentos listados a seguir são aprovados pela AC Raiz ou 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
[1]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[2]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[3]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICA DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[4]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[5]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[6]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

REF.	NOME DO DOCUMENTO	CÓDIGO
[7]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[8]	FORMULÁRIO DE REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO	ADE-ICP-01.A
[9]	SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC	ADE-ICP-01.B

11. Referências Bibliográficas

[*WebTrust Principles and Criteria for Registration Authorities*, disponível em http://www.webtrust.org.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 11.515/NB 1334: *Critérios de segurança física relativos ao armazenamento de dados*. 2007.

RFC 3647, IETF - *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, november 2003.

RFC 4210, IETF - *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, september 2005.

RFC 5019, IETF - *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*, september 2007
RFC 5280, IETF - *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, may 2008.
RFC 6712, IETF - *Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP)*, september 2012.
RFC 6960, IETF -X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.