



AC SAFEWEB JUS
POLÍTICA DE CERTIFICADO DE ASSINATURA – TIPO A3
Autor: Compliance
Edição: 28/06/2022
Versão: 1.0

safeweb
Você seguro e tranquilo na rede

POLÍTICA DE CERTIFICADO DE ASSINATURA - TIPO A3 DA AC SAFEWEB JUS

PC A3 - AC SAFEWEB JUS

Versão 1.0
Junho 2022



**AC SAFEWEB JUS
POLÍTICA DE CERTIFICADO DE ASSINATURA**

SUMÁRIO

1	INTRODUÇÃO.....	5
1.1	VISÃO GERAL	5
1.2	NOME DO DOCUMENTO E IDENTIFICAÇÃO	5
1.3	PARTICIPANTES DA ICP-BRASIL.....	5
1.4	USABILIDADE DO CERTIFICADO	7
1.5	POLÍTICA DE ADMINISTRAÇÃO	8
1.6	DEFINIÇÕES E ACRÔNIMOS	8
2	RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	9
3	IDENTIFICAÇÃO E AUTENTICAÇÃO	9
3.1	NOMEAÇÃO	10
3.2	VALIDAÇÃO INICIAL DE IDENTIDADE	10
3.3	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES.....	10
3.4	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO	10
4	REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	10
4.1	SOLICITAÇÃO DO CERTIFICADO	10
4.2	PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO	11
4.3	EMISSÃO DE CERTIFICADO	11
4.4	ACEITAÇÃO DE CERTIFICADO.....	11
4.5	USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO	11
4.6	RENOVAÇÃO DE CERTIFICADOS	11
4.7	NOVA CHAVE DE CERTIFICADO	12
4.8	MODIFICAÇÃO DE CERTIFICADO	12
4.9	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	12
4.10	SERVIÇOS DE STATUS DE CERTIFICADO	13
4.11	ENCERRAMENTO DAS ATIVIDADES	13
4.12	CUSTÓDIA E RECUPERAÇÃO DE CHAVE	13
5	CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES.....	13
5.1	CONTROLES FÍSICOS	13
5.2	CONTROLES PROCEDIMENTAIS	14
5.3	CONTROLES DE PESSOAL	14
5.4	PROCEDIMENTOS DE LOG DE AUDITORIA.....	14
5.5	ARQUIVAMENTO DE REGISTROS	14
5.6	TROCA DE CHAVE	15
5.7	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	15
5.8	EXTINÇÃO DA AC	15
6	CONTROLES TÉCNICOS DE SEGURANÇA.....	15
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	15



6.2	PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO ...	18
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	20
6.4	DADOS DE ATIVAÇÃO	20
6.5	CONTROLES DE SEGURANÇA COMPUTACIONAL.....	21
6.5.2	CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL	22
6.6	CONTROLES TÉCNICOS DO CICLO DE VIDA.....	22
6.7	CONTROLES DE SEGURANÇA DE REDE	23
6.8	CARIMBO DO TEMPO	23
7	PERFIS DE CERTIFICADO, LCR E OCSP	23
7.1	PERFIL DO CERTIFICADO	23
7.2	PERFIL DE LCR	30
7.3	PERFIL DE OCSP	30
8	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	31
8.1	FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES.....	31
8.2	IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR.....	31
8.3	RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA	31
8.4	TÓPICOS COBERTOS PELA AVALIAÇÃO.....	31
8.5	AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA.....	31
8.6	COMUNICAÇÃO DOS RESULTADOS	31
9	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	31
9.1	TARIFAS.....	31
9.2	RESPONSABILIDADE FINANCEIRA.....	31
9.3	CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO.....	31
9.4	PRIVACIDADE DA INFORMAÇÃO PESSOAL	31
9.5	DIREITO DE PROPRIEDADE INTELECTUAL.....	32
9.6	DECLARAÇÕES E GARANTIAS.....	32
9.7	ISENÇÃO DE GARANTIAS	32
9.8	LIMITAÇÕES DE RESPONSABILIDADES.....	32
9.9	INDENIZAÇÕES.....	32
9.10	PRAZO E RESCISÃO	32
9.11	AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES	32
9.12	ALTERAÇÕES	32
9.13	SOLUÇÃO DE CONFLITOS.....	33
9.14	LEI APLICÁVEL	33
9.15	CONFORMIDADE COM A LEI APLICÁVEL	33
9.16	DISPOSIÇÕES DIVERSAS	33
9.17	OUTRAS PROVISÕES	33
10	DOCUMENTOS REFERENCIADOS	33
11	REFERÊNCIAS BIBLIOGRÁFICAS.....	34



CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	28/06/2022	N/A	Versão Inicial



1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Esta Política de Certificado de Assinatura estabelece os requisitos observados pela AC Safeweb JUS, na emissão de seus certificados.

1.1.2 Esta Política de Certificado de Assinatura adota a mesma estrutura empregada no REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1].

1.1.3 A estrutura desta PC está baseada na RFC 3647.

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

1.1.5 O tipo de certificado de assinatura digital emitido sob essa PC é o Tipo A3.

1.1.6 Os certificados A3 de assinatura estão associados aos requisitos mais rigorosos de segurança.

1.1.7 Os certificados A3 de assinatura para Justiça podem ser emitidos para pessoas físicas (Cert-JUS Institucional, Cert-JUS Magistrado e Cert-JUS Poder Público).

1.1.8 Não se aplica.

1.1.9 Não se aplica.

1.1.10 Não se aplica.

1.1.11 Não se aplica.

1.1.12 Não se aplica.

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Esta Política de Certificado de Assinatura Digital é do tipo A3 da Autoridade Certificadora Safeweb para a Justiça, e referida como PC A3 da AC Safeweb JUS. O *Object Identifier* (OID) desta PC é **2.16.76.1.2.3.57**, atribuído na conclusão do processo de credenciamento da AC Safeweb JUS junto à ICP-Brasil.

1.2.2 Não se aplica.

1.3 PARTICIPANTES DA ICP-BRASIL

1.3.1 AUTORIDADES CERTIFICADORAS

1.3.1.1 Esta PC se refere à AC Safeweb JUS, integrante da ICP-Brasil, sob a hierarquia da Autoridade Certificadora da Justiça (AC JUS), que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira (AC Raiz).



1.3.1.2 As práticas e procedimentos de certificação da AC Safeweb JUS estão descritos na Declaração de Práticas de Certificação da AC Safeweb JUS (DPC da AC Safeweb JUS).

1.3.2 AUTORIDADES DE REGISTRO

1.3.2.1 Os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes são de competência das Autoridades de Registro (AR). As ARs vinculadas à AC Safeweb JUS estão relacionadas na página <https://safeweb.com.br/repositorio>, que contém:

- a) Relação de todas as ARs credenciadas;
- b) Relação de ARs que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3 TITULARES DO CERTIFICADO

1.3.3.1 Os certificados digitais **Cert-JUS Institucional**: destinam-se exclusivamente aos agentes públicos do Poder Judiciário, autorizados pela autoridade competente do seu órgão de lotação a recebê-los e identificam os titulares do certificado não só como indivíduo, mas também como servidor do órgão do Poder Judiciário em que está lotado.

1.3.3.2 Os certificados digitais **Cert-JUS Magistrado**: destinam-se exclusivamente aos MAGISTRADOS do Poder Judiciário, autorizados pela autoridade competente do seu atual órgão de atuação a recebê-los. Identificam os titulares não só como indivíduos, mas também como Magistrados do Poder Judiciário.

1.3.3.3 Os certificados digitais **Cert-JUS Poder Público**: destinam-se exclusivamente a agentes públicos, autorizados pela autoridade competente do seu órgão de lotação, a recebê-los. O certificado Cert-JUS Poder Público identifica o titular do certificado não só como indivíduo, mas também como servidor do órgão público em que está lotado, sendo vedada a emissão do Cert-JUS Poder Público para servidores de órgãos do Poder Judiciário.

1.3.4 PARTES CONFIÁVEIS

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

1.3.5 OUTROS PARTICIPANTES



A relação de todos os Prestadores de Serviços de Suporte (PSS), Prestadores de Serviços Biométricos (PSBios) e Prestadores de Serviço de Confiança (PSC), vinculados à AC Safeweb JUS estão relacionados na página <https://safeweb.com.br/repositorio>.

1.4 USABILIDADE DO CERTIFICADO

1.4.1 USO APROPRIADO DO CERTIFICADO

1.4.1.1 Os certificados definidos por esta Política de Certificado têm sua utilização vinculada à assinatura digital, não repúdio, garantia de integridade da informação e autenticação de seu titular.

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

1.4.1.3 A AC Safeweb JUS leva em conta o nível de segurança previsto para o tipo do certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado.

1.4.1.3.1 Os certificados Cert-JUS Institucional, Cert-JUS Magistrado e Cert-JUS Poder Público emitidos pela AC Safeweb JUS no âmbito desta PC serão utilizados nos atos praticados pelos agentes públicos no exercício de suas funções, tais como assinatura de documentos e mensagens de correio eletrônico, autenticação para acesso a sistemas e aplicações, login na rede e acesso remoto seguro.

1.4.1.3.2 Por ser instrumento de identificação pessoal e institucional bem como de assinatura digital pessoal do titular, o uso de tais certificados não é exclusivo para fins institucionais e profissionais, podendo ser utilizado para qualquer operação no meio digital que utilize a tecnologia de certificação digital.

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

1.4.1.5 Não se aplica.

1.4.1.6 Não se aplica.

1.4.1.7 Não se aplica.

1.4.1.8 Não se aplica.



1.4.2 USO PROIBITIVO DO CERTIFICADO

Não se aplica.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AC: AC Safeweb JUS

1.5.2 CONTATOS

Endereço: Av. Princesa Isabel, 828, Santana, Porto Alegre/RS, CEP 90620-000.

Telefone: +55 (51) 3018-0300

Página web: www.safeweb.com.br

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Roseli Zanquim

Telefone: +55 (51) 3018-0300

E-mail: compliance@safeweb.com.br

Outros: Setor de Governança & Compliance

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA PC

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

1.6 DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG ICP-BRASIL	Comitê Gestor da ICP-BRASIL
CN	<i>Common Name</i>
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro de Pessoas Físicas



CS	Code Signing
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SSL	Secure Socket Layer
UF	Unidade de Federação
URL	Uniform Resource Locator

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb JUS.

2.1 REPOSITÓRIOS

2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.4 CONTROLE DE ACESSO AOS REPOSITÓRIOS

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb JUS.



3.1 NOMEAÇÃO

- 3.1.1 Tipos de nomes
- 3.1.2 Necessidade dos nomes serem significativos
- 3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado
- 3.1.4 Regras para interpretação de vários tipos de nomes
- 3.1.5 Unicidade de nomes
- 3.1.6 Procedimento para resolver disputa de nomes
- 3.1.7 Reconhecimento, autenticação e papel de marcas registradas

3.2 VALIDAÇÃO INICIAL DE IDENTIDADE

- 3.2.1 Método para comprovar a posse de chave privada
- 3.2.2 Autenticação da identificação da organização
- 3.2.3 Autenticação da identidade de um indivíduo
- 3.2.4 Informações não verificadas do titular do certificado
- 3.2.5 Validação das autoridades
- 3.2.6 Critérios para interoperação
- 3.2.7 Autenticação da identidade de equipamento ou aplicação
- 3.2.8 Procedimentos complementares
- 3.2.9 Procedimentos específicos

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

- 3.3.1 Identificação e autenticação para rotina de novas chaves
- 3.3.2 Identificação e autenticação para novas chaves após a revogação

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb JUS.

4.1 SOLICITAÇÃO DO CERTIFICADO



- 4.1.1 Quem pode submeter uma solicitação de certificado
- 4.1.2 Processo de registro e responsabilidades

- 4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO**
- 4.2.1 Execução das funções de identificação e autenticação
- 4.2.2 Aprovação ou rejeição de pedidos de certificado
- 4.2.3 Tempo para processar a solicitação de certificado

- 4.3 EMISSÃO DE CERTIFICADO**
- 4.3.1 Ações da AC durante a emissão de um certificado
- 4.3.2 Notificações para o titular do certificado pela AC na emissão do certificado

- 4.4 ACEITAÇÃO DE CERTIFICADO**
- 4.4.1 Conduta sobre a aceitação do certificado
- 4.4.2 Publicação do certificado pela AC
- 4.4.3 Notificação de emissão do certificado pela AC Raiz para outras entidades

- 4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO**
- 4.5.1 Usabilidade da Chave privada e do certificado do titular
- 4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

- 4.6 RENOVAÇÃO DE CERTIFICADOS**
- 4.6.1 Circunstâncias para renovação de certificados
- 4.6.2 Quem pode solicitar a renovação
- 4.6.3 Processamento de requisição para renovação de certificados
- 4.6.4 Notificação para nova emissão de certificado para o titular
- 4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado
- 4.6.6 Publicação de uma renovação de um certificado pela AC
- 4.6.7 Notificação de emissão de certificado pela AC para outras entidades



4.7 NOVA CHAVE DE CERTIFICADO

- 4.7.1 Circunstâncias para nova chave de certificado
- 4.7.2 Quem pode requisitar a certificação de uma nova chave pública
- 4.7.3 Processamento de requisição de novas chaves de certificado
- 4.7.4 Notificação de emissão de novo certificado para o titular
- 4.7.5 Conduta constituindo a aceitação de uma nova chave certificada
- 4.7.6 Publicação de uma nova chave certificada pela AC
- 4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.8 MODIFICAÇÃO DE CERTIFICADO

- 4.8.1 Circunstâncias para modificação de certificado
- 4.8.2 Quem pode requisitar a modificação de certificado
- 4.8.3 Processamento de requisição de modificação de certificado
- 4.8.4 Notificação de emissão de novo certificado para o titular
- 4.8.5 Conduta constituindo a aceitação de uma modificação de certificado
- 4.8.6 Publicação de uma modificação de certificado pela AC
- 4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

- 4.9.1 Circunstâncias para revogação
- 4.9.2 Quem pode solicitar revogação
- 4.9.3 Procedimento para solicitação de revogação
- 4.9.4 Prazo para solicitação de revogação
- 4.9.5 Tempo em que a AC deve processar o pedido de revogação
- 4.9.6 Requisitos de verificação de revogação para as partes confiáveis
- 4.9.7 Frequência de emissão de LCR
- 4.9.8 Latência máxima para a LCR
- 4.9.9 Disponibilidade para revogação/verificação de status on-line
- 4.9.10 Requisitos para verificação de revogação on-line
- 4.9.11 Outras formas disponíveis para divulgação de revogação



- 4.9.12 Requisitos especiais para o caso de comprometimento de chave
- 4.9.13 Circunstâncias para suspensão
- 4.9.14 Quem pode solicitar suspensão
- 4.9.15 Procedimento para solicitação de suspensão
- 4.9.16 Limites no período de suspensão

4.10 SERVIÇOS DE STATUS DE CERTIFICADO

- 4.10.1 Características operacionais
- 4.10.2 Disponibilidade dos serviços
- 4.10.3 Funcionalidades operacionais

4.11 ENCERRAMENTO DAS ATIVIDADES

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

- 4.12.1 Política e práticas de custódia e recuperação de chave
- 4.12.2 Política e práticas de encapsulamento e recuperação de chave de sessão

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC da AC Safeweb JUS.

5.1 CONTROLES FÍSICOS

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



5.2 CONTROLES PROCEDIMENTAIS

- 5.2.1 Perfis qualificados
- 5.2.2 Número de pessoas necessário por tarefa
- 5.2.3 Identificação e autenticação para cada perfil
- 5.2.4 Funções que requerem separação de deveres

5.3 CONTROLES DE PESSOAL

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

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

- 5.4.1 Tipos de eventos registrados
- 5.4.2 Frequência de auditoria de registros
- 5.4.3 Período de retenção para registros de auditoria
- 5.4.4 Proteção de registros de auditoria
- 5.4.5 Procedimentos para cópia de segurança (Backup) de registros de auditoria
- 5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)
- 5.4.7 Notificação de agentes causadores de eventos
- 5.4.8 Avaliações de vulnerabilidade

5.5 ARQUIVAMENTO DE REGISTROS

- 5.5.1 Tipos de registros arquivados
- 5.5.2 Período de retenção para arquivo
- 5.5.3 Proteção de arquivo



- 5.5.4 Procedimentos de cópia de arquivo
- 5.5.5 Requisitos para datação de registros
- 5.5.6 Sistema de coleta de dados de arquivo (interno e externo)
- 5.5.7 Procedimentos para obter e verificar informação de arquivo

5.6 TROCA DE CHAVE

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

- 5.7.2 Recursos computacionais, software, e/ou dados corrompidos
- 5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade
- 5.7.4 Capacidade de continuidade de negócio após desastre

5.8 EXTINÇÃO DA AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São também definidos outros controles técnicos de segurança utilizados pela AC Safeweb JUS e pelas ARs vinculadas na execução de suas funções operacionais.

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1 O titular de certificado é a pessoa física responsável pela geração dos pares de chaves criptográficas.

6.1.1.1.1 Não se aplica.

6.1.1.1.2 Não se aplica.

6.1.1.2 A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante apresentados pelo browser ou componente disponibilizado pelo PSC envolvido na geração do par de chaves.



6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é o RSA, conforme definido no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.1.4 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme Tabela 2 a seguir.

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

6.1.1.6 O processo de geração do par de chaves assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

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

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

6.1.1.8 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL [3], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC Safeweb JUS, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

Tabela 2 – Mídias Armazenadoras de Chaves Criptográficas

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

Nota: Não se aplica.

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE

Não se aplica.



6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

A entrega da chave pública do solicitante do certificado é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - *Secure Socket Layer*.

6.1.4 ENTREGA DE CHAVE PÚBLICA DA AC SAFEWEB JUS ÀS TERCEIRAS PARTES

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

- a) No momento da disponibilização de um certificado para seu titular, usando formato definido no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil;
- b) Diretório;
- c) Página *web*:
 - c.1) Rep. 1: <http://repositorio.acsafeweb.com.br/ac-safewebjus/ac-safewebjus.p7b>
 - c.2) Rep. 2: <http://repositorio2.acsafeweb.com.br/ac-safewebjus/ac-safewebjus.p7b>
- d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil;
- e) Repositório da ICP-Brasil.

6.1.5 TAMANHOS DE CHAVE

6.1.5.1 O tamanho mínimo das chaves criptográficas associadas aos certificados da AC Safeweb JUS é de RSA 2048 bits para a hierarquia V5, conforme definido no DOC-ICP-01.01.

6.1.5.2 Os algoritmos e o tamanho de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados atendem ao padrão estabelecido no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.7 PROPÓSITOS DE USO DE CHAVE (CONFORME CAMPO "KEY USAGE" NA X.509 V3)



Os pares de chaves correspondentes aos certificados emitidos pela AC Safeweb JUS podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves. Para isso, os certificados emitidos segundo esta PC têm ativados os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment*.

6.2 PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

O repositório de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a) A chave privada é única e seu sigilo é suficientemente assegurado;
- b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros, pois é gerada em cartão, token ou HSM com certificação INMETRO. Esses módulos criptográficos não permitem a exportação da chave privada e exigem senha para a sua utilização.

6.2.1 PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1 O módulo criptográfico utilizado na geração e utilização de chaves criptográficas possui certificação INMETRO.

6.2.1.2 Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado seguem os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.2 CONTROLE "N DE M" PARA CHAVE PRIVADA

Não se aplica.

6.2.3 CUSTÓDIA (ESCROW) DE CHAVE PRIVADA

6.2.3.1 O agente de custódia (escrow) dos certificados emitidos pela AC Safeweb JUS, é o PSC Safeweb. As chaves privadas são armazenadas criptografadas em partições exclusivas em hardware criptográfico certificado pelo INMETRO. Estas chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e *push notification*).

6.2.3.2 A AC Safeweb JUS não implementa a recuperação de chaves privadas.



6.2.4 CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

6.2.4.1 Não se aplica.

6.2.4.2 A AC Safeweb JUS não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, no entanto em casos em que o CD é emitido utilizando o PSC Safeweb, a guarda da cópia da chave privada é realizada pelo próprio PSC.

6.2.4.3 Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico aprovado pelo DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4 Através das tecnologias atualmente disponíveis, o titular do certificado deve realizar a geração de cópia de segurança de sua chave privada, com os mesmos requisitos de segurança da chave original.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 As chaves privadas dos titulares de certificados emitidos por esta PC não são arquivadas.

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 AC Safeweb JUS gera os pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

6.2.7 ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Ver item 6.1.

6.2.8 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

A chave privada é ativada, mediante senha solicitada pelo software de proteção da chave privada. A senha deve ser criada e mantida apenas pelo titular do certificado, sendo para seu uso e conhecimento exclusivo. O titular de certificado deverá adotar senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 03 (três) meses.

6.2.9 MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA



A desativação da chave privada ocorre em função da expiração do certificado correspondente ou em função de sua revogação.

6.2.10 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

Para destruição da chave privada de certificados emitidos conforme esta PC, é preciso que o usuário acesse o software de proteção da chave privada, localize o certificado e o remova do repositório. A destruição da chave privada é irreversível e definitiva, não sendo mais possível a sua recuperação.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas da AC Safeweb JUS, dos titulares de certificados de assinatura digital e as LCRs por ela emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 PERÍODOS DE OPERAÇÃO DO CERTIFICADO E PERÍODOS DE USO PARA AS CHAVES PÚBLICA E PRIVADA

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

6.3.2.2 Não se aplica.

6.3.2.3 O período máximo de uso das chaves correspondentes aos certificados emitidos pela PC A3 da AC Safeweb JUS é de 5 (cinco) anos.

6.3.2.4 Não se aplica.

6.3.2.5 Não se aplica.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes desta PC estão descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO



6.4.1.1 Os certificados emitidos conforme esta PC, se utilizam de hardwares criptográficos para manter a segurança de suas chaves privadas. Estes hardwares possuem certificação INMETRO e protegem as chaves privadas armazenando-as em partições exclusivas para este fim, com acesso restrito apenas através da utilização de senha criada pelo próprio titular, não necessitando de outros dados de ativação para sua operação. Em casos de emissão através de PSC, as chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e *push notification*).

6.4.1.2 Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

6.4.2.1 Conforme descrito no item 6.4.1, os certificados emitidos conforme esta PC, não necessitam de dados de ativação para sua operação. Porém, para uma maior proteção, os titulares dos certificados podem utilizar recursos adicionais de segurança como a definição de senhas para utilização e exportação das chaves privadas. A configuração e utilização destes recursos adicionais de proteção fica a critério do titular do certificado. No caso de utilização de senha, recomenda-se:

- a) Nunca fornecer senha a terceiros;
- b) Escolher senhas de 08 (oito) ou mais caracteres;
- c) Definir senhas com caracteres numéricos e alfanuméricos;
- d) Memorizar a senha; e
- e) Não a escrever.

6.4.2.2 Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

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

Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Safeweb JUS, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

- a) Senha de *bios* ativada;
- b) Controle de acesso lógico ao sistema operacional;



- c) Exigência de uso de senhas fortes;
- d) Diretivas de senha e de bloqueio de conta;
- e) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;
- f) *Firewall* pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, *hotfix*, etc.);
- h) Proteção de tela acionada no máximo após 02 (dois) minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL

Não se aplica.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

A AC Safeweb JUS desenvolve sistemas relacionadas ao ciclo de vida do certificado digital, incluindo ferramentas de gestão de seu PSC.

6.6.1 CONTROLES DE DESENVOLVIMENTO DO SISTEMA

Como descrito no item correspondente da DPC da AC Safeweb JUS.

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

Como descrito no item correspondente da DPC da AC Safeweb JUS.

6.6.3 CONTROLES DE SEGURANÇA DE CICLO DE VIDA

Como descrito no item correspondente da DPC da AC Safeweb JUS.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

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



6.7 CONTROLES DE SEGURANÇA DE REDE

Não se aplica.

6.8 CARIMBO DO TEMPO

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

Os itens seguintes especificam os formatos dos certificados e das LCRs geradas segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1 PERFIL DO CERTIFICADO

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

7.1.1 NÚMERO DE VERSÃO

Todos os certificados emitidos pela AC Safeweb JUS, segundo esta PC, implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 EXTENSÕES DE CERTIFICADO

7.1.2.1 A AC Safeweb JUS implementa as mesmas extensões definidas como obrigatórias na ICP-Brasil, descritas no item 7.1.2.2

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

- a) "**Authority Key Identifier**", não crítica: o campo *keyIdentifier* contém o *hash* SHA-1 da chave pública da AC Safeweb JUS;
- b) "**Key Usage**", crítica: configurados conforme disposto no item 7.1.2.7 deste documento;
- c) "**Certificate Policies**", não crítica:
 - c.1) O campo *PolicyIdentifier* contém o OID desta PC: **2.16.76.1.2.3.57**;
 - c.2) O campo *PolicyQualifiers* contém o endereço *web* onde se obtém a DPC da AC Safeweb JUS: <http://repositorio.acsafeweb.com.br/ac-safewebjus/dpc->



[acsafewebjus.pdf](#).

d) "**CRL Distribution Points**", não crítica: contém o endereço na *web* onde se obtém a LCR correspondente:

d.1) Rep. 1: <http://repositorio.acsafeweb.com.br/ac-safewebjus/lcr-ac-safewebjus.crl>;

d.2) Rep. 2: <http://repositorio2.acsafeweb.com.br/ac-safewebjus/lcr-ac-safewebjus.crl>.

e) "**Authority Information Access**", não crítica: a primeira entrada contém o método de acesso *id-ad-calssuer*, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

e.1) Rep.1: <http://repositorio.acsafeweb.com.br/ac-safewebjus/ac-safewebjus.p7b>;

e.2) Rep. 2: <http://repositorio2.acsafeweb.com.br/ac-safewebjus/ac-safewebjus.p7b>.

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

A) PARA CERTIFICADO DE PESSOA FÍSICA (CERT-JUS INSTITUCIONAL, CERT-JUS MAGISTRADO E CERT-JUS PODER PÚBLICO):

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

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

II) OID = 2.16.76.1.3.6 e conteúdo: nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado.

III) OID = 2.16.76.1.3.5 e conteúdo: nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

a.2) campo *otherName*, não obrigatório, contendo:

I) OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo: Nome Principal que contém o domínio de login em estações de trabalho (UPN).



II) rfc822Name: contendo o e-mail institucional do responsável pelo certificado.
Este campo deverá estar no formato IA5string.

- b) Não se aplica.
- c) Não se aplica.
- d) Não se aplica.
- e) Não se aplica.

7.1.2.4 Os campos *otherName* definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

- a) O conjunto de informações definido em cada campo *otherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 *OCTET STRING* ou *PRINTABLE STRING*;
- b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
- c) Se o número do RG ou o número de inscrição do Título de Eleitor não estiver disponível, não se deve preencher os campos de órgão expedidor e UF ou os campos Zona Eleitoral, Sessão, Município e UF, respectivamente.
- d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;
- e) Todas as informações de tamanho variável referentes a números, tais como RG ou Título de Eleitor, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;
- f) As 10 (dez) posições das informações sobre órgão expedidor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;
- g) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;
- h) Não se aplica.



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

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

7.1.2.6.1 Nesta extensão o campo *otherName* com OID 2.16.76.1.3.1 deverá conter obrigatoriamente as informações Data de Nascimento, CPF e RG do titular.

7.1.2.6.2 Quando o <nome de login> for informado na AUTORIZAÇÃO, deve-se incluir um campo *otherName*, com OID=1.3.6.1.4.1.311.20.2.3, contendo User Principal Name (UPN) na forma usuário@domínio_institucional.

7.1.2.7 As extensões "*Key Usage*" e "*Extended Key Usage*" para os referidos tipos de certificado são obrigatórias e obedecem aos propósitos de uso e a criticalidade conforme descrição abaixo:

a) para os certificados de Assinatura e/ou Proteção de e-Mail:

"Key Usage", crítica: contém o *bit digitalSignature* ativado, podendo conter os *bits keyEncipherment* e *nonRepudiation* ativados;

"Extended Key Usage", não crítica: no mínimo um dos propósitos *client authentication* OID = 1.3.6.1.5.5.7.3.2 ou *E-mail protection* OID = 1.3.6.1.5.5.7.3.4 está ativado. Pode conter um campo "*SmartCardLogon*" (OID= 1.3.6.1.4.1.311.20.2.2) sempre que for solicitado e o UPN for fornecido.

7.1.3 IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC Safeweb JUS às entidades titulares de certificado são assinados com o uso do algoritmo RSA com SHA-256 como função de *hash* (OID = 1.2.840.113549.1.1.11), conforme o padrão PKCS#1.

7.1.4 FORMATOS DE NOME

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

7.1.4.1.1 Cert-JUS Institucional

I. O conteúdo do DN apresenta-se da seguinte forma para os certificados Cert-JUS Institucional:

C = BR

O = ICP-Brasil

OU = Autoridade Certificadora da Justica – AC-JUS



OU = AC Safeweb-JUS

OU = CNPJ da AR que realizou a identificação

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

OU = Cert-JUS Institucional – A3

OU = <Órgão de Lotação do Titular> - <Sigla do órgão>

OU = <Cargo do Titular>

CN = <Nome do Titular> : <#####>

7.1.4.1.1.1 Para o certificado Cert-JUS Institucional, exclusivo para o Poder Judiciário, a informação <Cargo do Titular> deverá ser preenchido SOMENTE com uma das seguintes opções:

- a) SERVIDOR/SERVIDORA;
- b) PRESTADOR DE SERVIÇO/PRESTADORA DE SERVIÇO; ou
- c) ESTAGIÁRIO/ESTAGIÁRIA.

7.1.4.1.2 Cert-JUS Magistrado

I. O conteúdo do DN apresenta-se da seguinte forma para os certificados Cert-JUS Magistrado:

C = BR

O = ICP-Brasil

OU = Autoridade Certificadora da Justiça – AC-JUS

OU = AC Safeweb-JUS

OU = CNPJ da AR que realizou a identificação

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

OU = Cert-JUS Magistrado – A3

OU = <Órgão de Lotação do Titular> = PODER JUDICIARIO

OU = <Cargo do Titular> = Magistrado/Magistrada

CN = <Nome do Titular> : <#####>

7.1.4.1.3 Cert-JUS Poder Público

I. O conteúdo do DN apresenta-se da seguinte forma para os certificados Cert-JUS Poder Público:

C = BR

O = ICP-Brasil

OU = Autoridade Certificadora da Justiça – AC-JUS

OU = AC Safeweb-JUS

OU = CNPJ da AR que realizou a identificação

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

OU = Cert-JUS Poder Público – A3

OU = <Órgão de Lotação do Titular> - <Sigla do órgão>



OU = <Cargo do Titular>

CN = <Nome do Titular> : <#####>

7.1.4.1.3.1 É vedada a emissão do Cert-JUS Poder Público para servidores de órgãos do Poder Judiciário.

7.1.4.2.5 Órgãos autorizados:

Órgãos não pertencentes ao Poder Judiciário deverão solicitar CADASTRAMENTO junto à AC-JUS, para a emissão de certificados Cert-JUS, sendo que a AC Safeweb JUS somente emitirá os certificados digitais para órgãos não pertencentes ao Poder Judiciário após o CADASTRAMENTO ter sido aprovado pela AC-JUS.

A lista de órgãos cadastrados, bem como as respectivas siglas padronizadas, está publicada no site da AC-JUS.

Em caso de dúvida sobre a padronização de nomes ou siglas de órgãos não constantes da lista publicada a unidade administrativa da AC-JUS deve ser consultada.

O cadastramento deve ser solicitado por ofício da autoridade competente do órgão interessado, endereçado à AC-JUS.

Após a aprovação do cadastro a AC-JUS oficiará as AC subsequentes para que incluam o órgão cadastrado nos seus sistemas de certificação. O nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente, conforme regras estabelecidas no item 4 e 5 do Leiaute da AC-JUS.

As AC da cadeia AC-JUS somente emitirão certificados digitais para órgãos não pertencentes ao Poder Judiciário após o CADASTRAMENTO ter sido aprovado pela AC-JUS.

Nota 1: Nos formatos listados anteriormente, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres “<” e “>” não devem ser incluídos.

Nota 2: Os caracteres “#” representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.

Nota 3: Os últimos nove caracteres do campo CN (Common Name) devem ser o nº de matrícula do titular no órgão de lotação, completado com caracteres brancos à direita, caso possua tamanho menor do que 9 caracteres.

Nota 4: Os dados necessários para preenchimento do DN deverão ser os informados na AUTORIZAÇÃO citada no item 3.1.9.1 ou 3.1.10.2 da DPC.

Nota 5: Todos os campos do DN são obrigatórios e devem ser preenchidos.



Nota 6: A lista contendo os nomes dos órgãos autorizados e respectivas siglas padronizadas está publicada no repositório da AC-JUS.

Nota 7: A AUTORIZAÇÃO citada no item 3.1.9.1 da DPC deverá conter também o UPN (nome de login do Window) na forma usuário@domínio_institucional, se for de interesse da instituição.

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. Não se aplica.

Nota: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5 RESTRIÇÕES DE NOME

7.1.5.1 Neste item estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

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

- Não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e
- Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)
Branco	20	+	2B
!	21	,	2C
“	22	-	2D
#	23	.	2E
\$	24	/	2F
%	25	:	3A
&	26	;	3B
'	27	=	3D
(28	?	3F
)	29	@	40
*	2A	\	5C

7.1.6 OID (OBJECT IDENTIFIER) DA PC

O OID (*Object Identifier*) desta PC é **2.16.76.1.2.3.57**. Todo certificado emitido segundo essa PC, contém o valor desse OID presente na extensão “*Certificate Policies*”.



7.1.7 USO DA EXTENSÃO "POLICY CONSTRAINTS"

Não se aplica.

7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Nos certificados emitidos segundo esta PC, o campo *policyQualifiers* da extensão "Certificate Policies" contém o endereço *web* da DPC AC Safeweb JUS: <http://repositorio.acsafeweb.com.br/ac-safewebjus/dpc-acsafewebjus.pdf>.

7.1.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS DE PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 PERFIL DE LCR

7.2.1 NÚMERO DE VERSÃO

As LCR geradas pela AC Safeweb 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 As extensões de LCR utilizadas pela AC Safeweb JUS são: "Authority Key Identifier" e "CRL Number", ambas consideradas não críticas, conforme descritas no item 7.2.2.2.

7.2.2.2 As LCRs da AC Safeweb JUS obedecem a ICP-Brasil que define como obrigatórias as seguintes extensões:

a) "**Authority Key Identifier**", **não crítica**: contém o *hash* SHA-1 da chave pública da AC Safeweb JUS que assina a LCR;

b) "**CRL Number**", **não crítica**: contém um número sequencial para cada LCR emitida pela AC Safeweb JUS.

7.3 PERFIL DE OCSP

7.3.1 NÚMERO DE VERSÃO

Não se aplica.

7.3.2 EXTENSÕES DE OCSP

Não se aplica.



8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb JUS.

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.5 AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

8.6 COMUNICAÇÃO DOS RESULTADOS

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Safeweb JUS.

9.1 TARIFAS

9.1.1 TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS

9.1.2 TARIFAS DE ACESSO AO CERTIFICADO

9.1.3 TARIFAS DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS

9.1.4 TARIFAS PARA OUTROS SERVIÇOS

9.1.5 POLÍTICA DE REEMBOLSO

9.2 RESPONSABILIDADE FINANCEIRA

9.2.1 COBERTURA DE SEGURO

9.2.2 OUTROS ATIVOS

9.2.3 COBERTURA DE SEGUROS OU GARANTIA PARA ENTIDADES FINAIS

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

9.3.2 INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

9.3.3 RESPONSABILIDADE EM PROTEGER A INFORMAÇÃO CONFIDENCIAL

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1 PLANO DE PRIVACIDADE

9.4.2 TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS



- 9.4.3 INFORMAÇÕES NÃO CONSIDERADAS PRIVADAS
- 9.4.4 RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADA
- 9.4.5 AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS
- 9.4.6 DIVULGAÇÃO EM PROCESSO JUDICIAL OU ADMINISTRATIVO
- 9.4.7 OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO

9.5 DIREITO DE PROPRIEDADE INTELECTUAL

9.6 DECLARAÇÕES E GARANTIAS

- 9.6.1 DECLARAÇÕES E GARANTIAS DA AC
- 9.6.2 DECLARAÇÕES E GARANTIAS DA AR
- 9.6.3 DECLARAÇÕES E GARANTIAS DO TITULAR
- 9.6.4 DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES
- 9.6.5 REPRESENTAÇÕES E GARANTIAS DE OUTROS PARTICIPANTES

9.7 ISENÇÃO DE GARANTIAS

9.8 LIMITAÇÕES DE RESPONSABILIDADES

9.9 INDENIZAÇÕES

9.10 PRAZO E RESCISÃO

- 9.10.1 PRAZO
- 9.10.2 TÉRMINO
- 9.10.3 EFEITO DA RESCISÃO E SOBREVIVÊNCIA

9.11 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

9.12 ALTERAÇÕES

As alterações serão realizadas conforme procedimentos de submissão, análise, aprovação e publicação que determina a Instrução Normativa nº 3 de 03 de abril de 2020.

9.12.1 PROCEDIMENTO PARA EMENDAS

A AC Safeweb JUS segue um processo periódico de atualização de suas PCs, que contempla a revisão em duas etapas. A primeira realizada pela equipe de Compliance/ Segurança da Informação e a segunda pela aprovação da Diretoria, visando a adequação dos documentos conforme as normas, procedimentos e regulamentos atuais da AC JUS e ICP-Brasil. Qualquer alteração nesta PC será submetida à aprovação da AC Raiz.



9.12.2 MECANISMO DE NOTIFICAÇÃO E PERÍODOS

A AC Safeweb JUS mantém a versão corrente desta PC para consulta pública em seu repositório web, no endereço: <http://repositorio.acsafeweb.com.br/ac-safewebjus/pc-a3-acsafewebjus.pdf>.

9.12.3 CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO

9.13 SOLUÇÃO DE CONFLITOS

9.14 LEI APLICÁVEL

9.15 CONFORMIDADE COM A LEI APLICÁVEL

9.16 DISPOSIÇÕES DIVERSAS

9.16.1 ACORDO COMPLETO

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

9.16.2 CESSÃO

9.16.3 INDEPENDÊNCIA DE DISPOSIÇÕES

9.16.4 EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)

9.17 OUTRAS PROVISÕES

Esta PC foi submetida à aprovação, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2]. Como parte desse processo, além da conformidade com este documento, é verificada a compatibilidade entre a PC e a DPC da AC Safeweb JUS.

10 DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL. Aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.	DOC-ICP-04



[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL. Aprovado pela Resolução CG ICP-Brasil nº 178, de 20 de outubro de 2020.	DOC-ICP-03
[3]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL. Aprovado pela Resolução CG ICP-Brasil nº 180, de 20 de outubro de 2020.	DOC-ICP-17

11 REFERÊNCIAS BIBLIOGRÁFICAS

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

RFC 5280, IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, may 2008.