DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS DA AR ARALINK CERTIFICAÇÃO DIGITAL

vinculada à AC SAFEWEB CD

DPN – AR ARALINK CERTIFICAÇÃO DIGITAL

Versão 1.0

Agosto 2023

Rua José Domingues Pereira, nº 877, Sala 1., bairro Ouro Verde
Campo Largo / PR/ Brasil– CEP 83.606-210
CNPJ 30.975.170/0001-52 | Site https://www.aralinkcertificadodigital.com.br/

AR ARALINK CERTIFICAÇÃO DIGITAL

DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS

SUMÁRIO

1 INTRODUÇÃO 6
1.1 VISÃO GERAL 6
1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO 6
1.3 PARTICIPANTES DA ICP-BRASIL 6
1.4 USABILIDADE DO CERTIFICADO 7
1.5 POLÍTICA DE ADMINISTRAÇÃO 8
1.6 DEFINIÇÕES E ACRÔNIMOS 9
2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 10
2.1 REPOSITÓRIOS 10
2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS 10
2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO 11
2.4 CONTROLE DE ACESSO AOS REPOSITÓRIOS 11
3 IDENTIFICAÇÃO E AUTENTICAÇÃO 11
3.1 ATRIBUIÇÃO DE NOMES 11
3.2 VALIDAÇÃO INICIAL DE IDENTIDADE 12
3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES 19
4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 21
4.1 SOLICITAÇÃO DE CERTIFICADO 21
4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO 24
4.3 EMISSÃO DE CERTIFICADO 24
4.4 ACEITAÇÃO DO CERTIFICADO 25
4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO 25
4.6. RENOVAÇÃO DE CERTIFICADOS 26
4.7 NOVA CHAVE DE CERTIFICADO (RE-KEY) 27
4.8 MODIFICAÇÃO DE CERTIFICADO 27
4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO 27
4.10 SERVIÇOS DE STATUS DE CERTIFICADO 31
4.11 ENCERRAMENTO DE ATIVIDADES 31
4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE 32
5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL 32
5.1 CONTROLES FÍSICOS 32
5.2 CONTROLES PROCEDIMENTAIS 34
5.3 CONTROLES DE PESSOAL 34
5.4 PROCEDIMENTOS DE LOG DE AUDITORIA 37
5.5 ARQUIVAMENTO DE REGISTROS 38

5.6 TROCA DE CHAVE 38
5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE 39
5.8 EXTINÇÃO DA AC 39
6 CONTROLES TÉCNICOS DE SEGURANÇA 39
6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES 39
6.2 PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO 41
6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES 42
6.4 DADOS DE ATIVAÇÃO 42
6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL 43
6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA 46
6.7 CONTROLES DE SEGURANÇA DE REDE 47
6.8 CARIMBO DO TEMPO 47
7 PERFIS DE CERTIFICADO, LCR E OCSP 47
7.1 PERFIL DO CERTIFICADO 47
7.2 PERFIL DE LCR 48
7.3 PERFIL DE OCSP 49
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES 49
8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES 49
8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR 49
8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA 49
8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO 49
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 50
9.2 RESPONSABILIDADE FINANCEIRA 51
9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO 51
9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL 53
9.5 DIREITO DE PROPRIEDADE INTELECTUAL 54
9.6 DECLARAÇÕES E GARANTIAS 54
9.7 ISENÇÃO DE GARANTIAS 55
9.8 LIMITAÇÕES DE RESPONSABILIDADES 55
9.9 INDENIZAÇÕES 55
9.10 PRAZO E RESCISÃO 55
9.11 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES 56
9.12 ALTERAÇÕES 56
9.13 SOLUÇÃO DE CONFLITOS 56
9.14 LEI APLICÁVEL 57
9.15 CONFORMIDADE COM A LEI APLICÁVEL 57

9.16 DISPOSIÇÕES DIVERSAS 57
9.17 OUTRAS PROVISÕES 57
10 DOCUMENTOS REFERENCIADOS 58
10.1 RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-BRASIL 58
10.2 INSTRUÇÕES NORMATIVAS DA AC RAIZ 58
10.3 APROVAÇÕES DA AC RAIZ 58
11 REFERÊNCIAS BIBLIOGRÁFICAS 59

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	31/08/2023	N/A	Versão inicial

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Esta Declaração de Práticas de Negócios (DPN), constitui os requisitos mínimos, obrigatoriamente observados pela Autoridade de Registro **AR ARALINK CERTIFICAÇÃO DIGITAL** , integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), vinculada à Autoridade Certificadora Safeweb CD (AC SAFEWEB CD) e descreve as práticas e os procedimentos utilizados por esta AR na execução de seus serviços.

1.1.2 Esta DPN adota a mesma estrutura utilizada no DOC-ICP-05, que estabelece os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [5].

1.1.3 Não se aplica.

1.1.4 A estrutura desta DPN está baseada na RFC 3647.

1.1.5 A **AR ARALINK CERTIFICAÇÃO DIGITAL** mantém todas as informações da sua DPN sempre atualizadas

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Este documento é chamado “Declaração de Práticas de Negócios da **AR ARALINK CERTIFICAÇÃO DIGITAL** ”, referido a seguir simplesmente como "DPN - **AR ARALINK CERTIFICAÇÃO DIGITAL** " e descreve as práticas e os procedimentos empregados pela **AR ARALINK CERTIFICAÇÃO DIGITAL** no âmbito da ICP-Brasil.

1.2.2 Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados cujas solicitações de emissão são recebidas, validadas e encaminhadas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** para a AC SAFEWEB CD são: assinatura de documento e proteção de e-mail (S/MIME).

1.3 PARTICIPANTES DA ICP-BRASIL

1.3.1 AUTORIDADE CERTIFICADORA - AC

A **AR ARALINK CERTIFICAÇÃO DIGITAL** está vinculada à AC SAFEWEB CD, que está no nível imediatamente subsequente ao da Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC RFB), que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira. Com relação aos tipos de certificados emitidos pela AC SAFEWEB CD, devem ser observadas as suas Políticas de Certificados (PC), que explicam como os certificados são gerados, administrados pela AC SAFEWEB CD e utilizados pela comunidade.

1.3.2 AUTORIDADE DE REGISTRO - AR

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 CD estão relacionadas na página https://www.safeweb.com.br/repositorio que contém as seguintes informações:

a) relação de todas as AR credenciadas;

b) relação de AR que tenha se descredenciado da cadeia da AC SAFEWEB CD, com respectivas datas do descredenciamento.

1.3.3 TITULARES DE CERTIFICADO

Podem ser titulares de certificados cujas solicitações de emissão são recebidas, validadas e encaminhadas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** para a AC SAFEWEB CD, pessoas físicas inscritas no CPF, desde que não enquadradas na situação cadastral de CANCELADA ou NULA, e pessoas jurídicas inscritas no CNPJ, desde que não enquadradas na condição de NULA conforme o disposto nos incisos I e II do art. 6° da Instrução Normativa RFB n° 1077, de 29 de Outubro de 2010 e Anexo I da Portaria RFB/Sucor/Cotec nº 18, de 19 de fevereiro de 2019 (Leiaute dos Certificados Digitais da Secretaria da Receita Federal do Brasil - Versão 4.4). Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será o detentor da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrada no CNPJ da Receita Federal do Brasil. Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

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

Os Prestadores de Serviços de Suporte (PSS), Prestadores de Serviços Biométricos (PSBio) e os Prestadores de Serviço de Confiança (PSC), vinculados à AC SAFEWEB CD, estão relacionados na página https://www.safeweb.com.br/repositorio.

1.4 USABILIDADE DO CERTIFICADO

1.4.1 USO APROPRIADO DO CERTIFICADO

A **AR ARALINK CERTIFICAÇÃO DIGITAL** realiza os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes

para a AC SAFEWEB CD, conforme as seguintes Políticas de Certificado Digital:

Política de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da AC SAFEWEB CD	PC A1-AC SAFEWEB CD	2.16.76.1.2.1.51
Política de Certificado de Assinatura Digital tipo A3 da AC SAFEWEB CD	PC A3-AC SAFEWEB CD	2.16.76.1.2.3.48

As PCs correspondentes relacionam as aplicações para as quais são adequados os certificados cujas solicitações de emissão são recebidas, validadas e encaminhadas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD.

1.4.2 USO PROIBITIVO DO CERTIFICADO

Quando cabível, as aplicações para as quais existem restrições ou proibições para o uso desses certificados estão listadas nas PCs correspondentes.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AR : **AR ARALINK CERTIFICAÇÃO DIGITAL**

1.5.2 CONTATOS

Endereço: Rua José Domingues Pereira, nº 877, Sala 1, Bairro Ouro verde, Campo Largo/PR – CEP: 83.606-210
Telefone: (41) 3292-1001
Página web: https://www.aralinkcertificadodigital.com.br/
E-mail: LEOPOLDO@KAYSER.COM.BR

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPN COM A DPC

Nome: LEOPOLDO JOAO KAYSER NETO
Telefone: (41) 3292-1001
E-mail: LEOPOLDO@KAYSER.COM.BR

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA DPN

Esta DPN não necessita ser submetida, nem aprovada pelo ITI.

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*
CMVP	*Cryptographic Module Validation Program*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	*Comitee of Sponsoring Organizations*
CPF	Cadastro de Pessoas Físicas
CS	*Code Signing*
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	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	*National Institute of Standards and Technology*
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
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

PIS	Programa de Integração Social
POP	*Proof of Possession*
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	*Simple Network Management Protocol*
SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 REPOSITÓRIOS

2.1.1 As obrigações da AC SAFEWEB CD em relação ao seu repositório estão descritas no item correspondente de sua DPC.

2.1.2 Os requisitos aplicáveis aos repositórios utilizados pela AC SAFEWEB CD, estão descritas no item correspondente de sua DPC.

2.1.3 A disponibilidade do repositório da AC SAFEWEB CD está descrita no item correspondente de sua DPC.

2.1.4 Os endereços dos repositórios da AC SAFEWEB CD estão descritos no item correspondente de sua DPC.

2.1.5 As obrigações da **AR ARALINK CERTIFICAÇÃO DIGITAL** em relação ao seu repositório estão abaixo relacionadas:

a) Publicar a sua DPN em sua página de internet;

b) Possuir um domínio de internet registrado sob o CNPJ da entidade credenciada na ICP-Brasil.

2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.2.1 A disponibilidade do repositório da AC SAFEWEB CD está descrita no item correspondente de sua DPC.

2.2.2 As informações publicadas pela AC SAFEWEB CD em página web estão descritas no item correspondente de sua DPC.

2.2.3 As seguintes informações, no mínimo, são publicadas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** em página web:

a) Sua Declaração de Práticas de Negócio.

2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.3.1 Certificados cujas solicitações de emissão são recebidas, identificadas e encaminhadas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, são publicados imediatamente após sua emissão.

2.3.3 As versões ou alterações desta DPN são atualizadas no site da **AR ARALINK CERTIFICAÇÃO DIGITAL** .

2.4 CONTROLE DE ACESSO AOS REPOSITÓRIOS

Não existe qualquer restrição de acesso para consulta a esta DPN.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A **AR ARALINK CERTIFICAÇÃO DIGITAL** verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes de encaminhar as solicitações de certificados digitais para a AC SAFEWEB CD. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os direitos de propriedade intelectual de terceiros. A **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 A **AR ARALINK CERTIFICAÇÃO DIGITAL** encaminha solicitações de emissão de certificados recebidas para a AC SAFEWEB CD, com nomes que possibilitam determinar a identidade da pessoa ou organização a que se referem. Para tanto utiliza o "D*istinguished Name*" do padrão ITU X.500, seguindo os padrões estabelecidos pelo documento LEIAUTE DOS CERTIFICADOS DIGITAIS DA SECRETARIA DA RECEITA FEDERAL DO BRASIL [14]. Informações específicas, estão descritas nas PC implementadas, no item 7.1.4.

3.1.1.2 Não se aplica.

3.1.2 NECESSIDADE DOS NOMES SEREM SIGNIFICATIVOS

3.1.2.1 As solicitações de certificados encaminhadas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC

SAFEWEB CD fazem uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem, para a identificação dos titulares dos certificados emitidos pela AC SAFEWEB CD.

3.1.2.2 Para certificados de pessoa física (e-CPF), o campo *Common Name* é composto do nome do Titular do Certificado, conforme consta no Cadastro de Pessoa Física (CPF).

3.1.2.3 Para os certificados de pessoa jurídica (e-CNPJ), o campo *Common Name* é composto do nome empresarial da pessoa jurídica, conforme consta no Cadastro Nacional de Pessoa Jurídica (CNPJ).

3.1.3 ANONIMATO OU PSEUDÔNIMO DOS TITULARES DO CERTIFICADO

Não se aplica.

3.1.4 REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES

Não se aplica.

3.1.5 UNICIDADE DE NOMES

Os identificadores do tipo "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC SAFEWEB CD. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo. Para assegurar a unicidade do campo, no certificado de pessoa física (e-CPF) é incluído o número do CPF após o nome do titular do certificado e, no certificado de pessoa jurídica (e-CNPJ), é incluído o número do CNPJ.

3.1.6 PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

Para a **AR ARALINK CERTIFICAÇÃO DIGITAL** não há disputa de nomes entre solicitantes de certificados, uma vez que o nome será obtido a partir dos dados da Receita Federal do Brasil, CPF ou CNPJ para certificados de pessoa física ou jurídica, respectivamente, acrescido do número de inscrição, o que garante a unicidade de todos os nomes no âmbito da AC SAFEWEB CD.

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

A **AR ARALINK CERTIFICAÇÃO DIGITAL** utiliza os procedimentos e os requisitos para a primeira identificação e cadastramento junto à ICP-Brasil de pessoas físicas titulares ou responsáveis por certificados

digitais, compreendendo os seguintes processos:

a) identificação e cadastro iniciais do titular do certificado – identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7, observado o quanto segue:

I. para certificados de pessoa física: comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e biometrias apresentadas, vedada qualquer espécie de procuração para tal fim.

II. para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa física 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.

b) emissão do certificado: após a conferência dos dados da solicitação de certificado com os constantes dos documentos e biometrias apresentados, na etapa de identificação, é liberada a emissão do certificado no sistema da AC SAFEWEB CD. A extensão *Subject Alternative Name* é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

3.2.1 MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA

A **AR ARALINK CERTIFICAÇÃO DIGITAL** utiliza um teste de assinatura, durante a solicitação do certificado, como método para verificar se o requerente do certificado possui a posse da chave privada. Neste teste, é realizado um processo de assinatura com a chave privada, enquanto a chave pública (certificado assinado pela autoridade certificadora) é utilizada para verificar a validade desta assinatura. No caso em que sejam requeridos procedimentos específicos para as PCs implementadas, eles são descritos nessas PCs, no item correspondente.

3.2.2 AUTENTICAÇÃO DA IDENTIFICAÇÃO DA ORGANIZAÇÃO

3.2.2.1 DISPOSIÇÕES GERAIS

3.2.2.1.1 A confirmação da identidade de uma pessoa jurídica é feita mediante consulta às bases de dados da RFB e mediante a presença física do interessado ou por meio de videoconferência, conforme requisitos do DOC-ICP-05.05 e regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, com base em documentos de identificação legalmente aceitos e pelo processo de identificação biométrica da ICP-Brasil.

3.2.2.1.2 Será designado como responsável pelo certificado o representante legal da pessoa jurídica requerente do certificado, ou o procurador constituído na forma do item 3.2, alínea 'a', inciso (ii) acima, o qual será o detentor da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrado no CNPJ da RFB.

3.2.2.1.3 A **AR ARALINK CERTIFICAÇÃO DIGITAL** realiza a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) Apresentação do rol de documentos elencados no item 3.2.2.2;

b) Apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1; c) Coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil, bem como os procedimentos para identificação biométrica na ICP-Brasil; e

d) Assinatura digital do termo de titularidade de que trata o item 4.1 pelo titular ou responsável pelo uso do certificado.

Nota 1: A **AR ARALINK CERTIFICAÇÃO DIGITAL** poderá solicitar uma assinatura manuscrita ao requerente ou responsável pelo uso do certificado em termo específico para a comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

3.2.2.1.4 Fica dispensado o disposto no item 3.2.2.1.3, alíneas "b" e "c" caso o responsável pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial. 3.2.2.1.5 O disposto no item 3.2.2.1.3 poderá ser realizado:

a) Mediante comparecimento presencial do responsável pelo certificado; ou

b) Por videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

3.2.2.2 DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

Durante a solicitação de certificado e-CNPJ é realizada consulta à situação cadastral do CNPJ junto ao cadastro da Receita Federal do Brasil. Se o CNPJ estiver INAPTO, SUSPENSO, BAIXADO ou NULO - situações que impedem o fornecimento do certificado - a solicitação não poderá ser enviada pela **AR ARALINK**

CERTIFICAÇÃO DIGITAL à AC SAFEWEB CD. A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos à sua habilitação jurídica:

I – Se pessoa jurídica criada ou autorizada a sua criação por lei:

1) Cópia do CNPJ.

II – Se entidade privada:

1) Certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e

2) Documentos da eleição de seus administradores, quando aplicável.

b) Relativos à sua habilitação fiscal:

I - Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ); ou

II - Prova de inscrição no Cadastro Específico do INSS (CEI).

Nota 1: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

3.2.2.3 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO

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

a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);

c) Nome completo do responsável pelo certificado, sem abreviações; e

d) Data de nascimento do responsável pelo certificado.

3.2.2.3.2 Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o responsável pelo certificado poderá, a seu critério e mediante declaração expressa no termo de titularidade, solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.2.3.2.

3.2.2.4 RESPONSABILIDADE DECORRENTE DO USO DO CERTIFICADO DE UMA ORGANIZAÇÃO

Os atos praticados com o certificado digital de titularidade de uma organização estão sujeitos ao regime de responsabilidade definido em lei quanto aos poderes de representação conferidos ao responsável indicado no certificado.

3.2.3 AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO

Durante a solicitação dos certificados e-CPF é realizada consulta da situação cadastral do solicitante mediante número de CPF cadastrado através da RFB e consultado nesta base, conforme art. 6º da Instrução Normativa SRF N° 222. Se o CPF informado for inexistente ou se a pessoa física apresentar a condição de CANCELADA ou NULA, a solicitação não será enviada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD.

A confirmação da identidade é realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos ou por meio de videoconferência, conforme procedimentos e requisitos técnicos do DOC-ICP-05.05, definidos em Instrução Normativa da AC Raiz. Os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

3.2.3.1 DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

A identificação da pessoa física requerente do certificado deverá ser realizada como segue:

a) Apresentação da seguinte documentação, em sua versão original oficial, física ou digital:

I. Registro de Identidade, se brasileiro; ou

II. Título de Eleitor, com foto; ou

III. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou

IV. Passaporte, se estrangeiro não domiciliado no Brasil.

b) Coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

Nota 1: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

Nota 2: A **AR ARALINK CERTIFICAÇÃO DIGITAL** reserva-se ao direito de somente aceitar a apresentação da Carteira de Trabalho e Previdência Social (CTPS) em complementação ao primeiro documento de identificação apresentado. A aceitabilidade da CTPS como documento único de identificação para emissão do Certificado Digital deverá passar por análise e parecer da AC SAFEWEB CD.

Nota 3: Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

Nota 4: Os documentos que possuem data de validade precisam estar dentro do prazo. Excepcionalmente,

a CNH vencida poderá ser aceita para identificação de titular de certificado digital.

Nota 5: O e-mail de comunicação fornecido, deve ser exclusivo e obrigatório do titular do CD, para garantia da integridade e segurança das informações prestadas.

3.2.3.1.1 Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a apresentação de qualquer dos documentos elencados no item 3.2.3.1 e a etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

3.2.3.1.2 Os documentos digitais deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos. Tal verificação fará parte do dossiê eletrônico do titular do certificado. Na hipótese da identificação positiva, fica dispensada a etapa de verificação conforme o item 3.2.3.1.3.

3.2.3.1.3 Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados:

a) por agente de registro distinto do que realizou a etapa de identificação;

b) na sede da **AR ARALINK CERTIFICAÇÃO DIGITAL** ou AR própria da AC SAFEWEB CD; e

c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.2.3.1.4 A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente, e as normas editadas pelo Comitê Gestor da ICP-Brasil.

3.2.3.1.5 Não se aplica.

3.2.3.1.6 Não se aplica.

3.2.3.1.7 Não se aplica.

3.2.3.1.8 A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICP-Brasil, que deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade.

3.2.3.2 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

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

a) Nome completo, sem abreviações;

b) CPF;

c) Data de nascimento;

d) E-mail.

3.2.3.2.2 Cada PC da AC SAFEWEB CD pode definir como obrigatório o preenchimento de outros campos ou o titular do certificado poderá, a seu critério e mediante declaração expressa no termo de titularidade,

solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

a) Número de Identificação Social - NIS (PIS, PASEP ou CI);

b) Número do Registro Geral - RG do titular e órgão expedidor;

c) Número do Cadastro Específico do INSS (CEI);

d) Número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;

e) Número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente;

3.2.3.2.3 Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original.

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

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

3.2.4 INFORMAÇÕES NÃO VERIFICADAS DO TITULAR DO CERTIFICADO

Não se aplica.

3.2.5 VALIDAÇÃO DAS AUTORIDADES

Não se aplica.

3.2.6 CRITÉRIOS PARA INTEROPERAÇÃO

Não se aplica.

3.2.7 AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO OU APLICAÇÃO

Não se aplica.

3.2.8 PROCEDIMENTOS COMPLEMENTARES

3.2.8.1 A **AR ARALINK CERTIFICAÇÃO DIGITAL** mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos do documento Princípios e Critérios *WebTrust* para AR [15].

3.2.8.2 Todo o processo de identificação do titular do certificado é registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC SAFEWEB CD

e utilizada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** , com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. O sistema biométrico da ICP-Brasil solicita aleatoriamente qual dedo o AGR deve apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGR no cadastro do sistema biométrico. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.2.8.3 Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no DOC-ICP 03.01, regulamento editado por instrução normativa da AC Raiz que define as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.1 Não se aplica.

3.2.8.4 A AC SAFEWEB CD disponibiliza à **AR ARALINK CERTIFICAÇÃO DIGITAL** , uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02, regulamento editado por instrução normativa da AC Raiz que define os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil.

3.2.8.4.1 Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, poderá ser dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação conforme item 3.2.3.1.

3.2.9 PROCEDIMENTOS ESPECÍFICOS

3.2.9.1 Não se aplica.

3.2.9.2 Não se aplica.

3.2.9.3 Não se aplica.

3.2.9.4 Não se aplica.

3.2.9.5 Não se aplica.

3.2.9.6 Não se aplica.

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1 Esta DPN estabelece os processos de identificação e confirmação do cadastro do solicitante, utilizados pela **AR ARALINK CERTIFICAÇÃO DIGITAL** e pela AC SAFEWEB CD para a geração de novo par de chaves e de seu correspondente novo certificado.

3.3.2 Esse processo será conduzido conforme uma das seguintes possibilidades:

a) Adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2, 3.2.3 ou 3.2.7;

b) Solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;

c) Solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;

d) Solicitação por meio eletrônico dada nas alíneas 'b' e 'c', acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme requisitos do DOC-ICP-05.05, regulamentação a ser editada pela AC Raiz, ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;

e) Por meio de videoconferência, conforme procedimentos e requisitos técnicos do DOCICP-05.05, definidos em Instrução Normativa da AC Raiz, os quais asseguram nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou

f) Não se aplica.

3.3.2.1 Não se aplica.

3.3.3 Caso sejam requeridos procedimentos específicos para as PC implementadas, os mesmos serão descritos nessas PC, no item correspondente.

3.3.4 Não se aplica.

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

3.4.1 A solicitação de revogação de certificado é realizada através de formulário específico ou página web, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita através da confrontação de dados fornecidos no momento da solicitação de revogação, com os dados previamente cadastrados na **AR ARALINK CERTIFICAÇÃO DIGITAL** . O item 4.9.2 desta DPN descreve quem pode solicitar a revogação de um certificado.

3.4.2 Os procedimentos para solicitação de revogação de certificado estão descritos no item 4.9.3 desta DPN. As solicitações de revogação de certificados são obrigatoriamente documentadas.

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 SOLICITAÇÃO DE CERTIFICADO

A solicitação de emissão de um Certificado Digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela **AR ARALINK CERTIFICAÇÃO DIGITAL** . Toda referência a formulário deverá ser entendida também como referência a outras formas que a **AR ARALINK CERTIFICAÇÃO DIGITAL** possa vir a adotar. Dentre os requisitos e procedimentos operacionais estabelecidos pela **AR ARALINK CERTIFICAÇÃO DIGITAL** para as solicitações de emissão de certificado, estão:

a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.2;

b) O uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado do tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; e

c) Um termo de titularidade e responsabilidade deverá ser assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico.

Nota: Na impossibilidade técnica de assinatura digital do termo de titularidade será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo uso do certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

4.1.1 QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO

A submissão da solicitação deve ser sempre por intermédio da AR vinculada, através de agente de registro devidamente autorizado. Para certificados de pessoa física, a solicitação deve ser feita pelo próprio titular, e no caso de pessoa jurídica, deve ser feita pelo representante legal.

4.1.1.1 Não se aplica.

4.1.1.2 Não se aplica.

4.1.1.3 Não se aplica.

4.1.1.4 Não se aplica.

4.1.2 PROCESSO DE REGISTRO E RESPONSABILIDADES

Nos itens a seguir são descritas as obrigações gerais das entidades envolvidas. As obrigações específicas, quando aplicáveis, estão descritas nas PCs implementadas.

4.1.2.1 Responsabilidades da AC SAFEWEB CD

4.1.2.1.1 A AC SAFEWEB CD responde pelos danos a que der causa.

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

4.1.2.1.3 Não se aplica

4.1.2.2 Obrigações da AC SAFEWEB CD

a) operar de acordo com a sua DPC e com as PCs que implementa;

b) gerar e gerenciar os seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC Secretaria da Receita Federal do Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, 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 AR a ela vinculadas e de usuários finais;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas LCRs;

k) publicar em sua página web sua DPC e as PCs aprovadas que implementa;

l) publicar, em sua página web, as informações definidas no item 2.2.2 de sua DPC;

m) publicar, em página web, informações sobre o descredenciamento de AR;

n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;

o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas 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 anualmente seu Plano de Continuidade do Negócio (PCN);

t) manter 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, de acordo com as normas do CG da ICP-Brasil;

u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;

v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;

w) não emitir certificado 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) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados.

4.1.2.3 Responsabilidades da AR ARALINK CERTIFICAÇÃO DIGITAL

A **AR ARALINK CERTIFICAÇÃO DIGITAL** será responsável pelos danos a que der causa.

4.1.2.4 Obrigações da AR ARALINK CERTIFICAÇÃO DIGITAL

A **AR ARALINK CERTIFICAÇÃO DIGITAL** têm as seguintes obrigações:

a) Receber solicitações de emissão ou de revogação de certificados;

b) Confirmar a identidade do solicitante e a validade da solicitação;

c) Encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC SAFEWEB CD, utilizando protocolo de comunicação seguro, conforme padrão definido no DOC-ICP-03.01, regulamento editado por instrução normativa da AC Raiz que define as características mínimas de segurança para as AR da ICP-Brasil;

d) Informar aos respectivos titulares a emissão ou a revogação de seus certificados;

e) Manter a conformidade dos seus processos, procedimentos e atividades com as normas,

critérios, práticas e regras estabelecidas pela AC SAFEWEB CD e pela ICP-Brasil, em especial com o contido DOC-ICP-03.01, regulamento editado por instrução normativa da AC Raiz que define as características mínimas de segurança para as AR da ICP-Brasil, bem como Princípios e Critérios *WebTrust* para AR [15];

f) Manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);

g) Proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2, 3.2.3 e 3.2.7; e

h) Divulgar suas práticas, relativas à cadeia da AC SAFEWEB CD, em conformidade com o documento Princípios e Critérios *WebTrust* para AR [15].

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1 EXECUÇÃO DAS FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO

A **AR ARALINK CERTIFICAÇÃO DIGITAL** executa as funções de identificação e autenticação conforme item 3 desta DPN.

4.2.2 APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO

4.2.2.1 Não se aplica.

4.2.2.2 A **AR ARALINK CERTIFICAÇÃO DIGITAL** pode, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPN.

4.2.3 TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO

A **AR ARALINK CERTIFICAÇÃO DIGITAL** e a AC SAFEWEB CD cumprem 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 SAFEWEB CD DURANTE A EMISSÃO DE UM CERTIFICADO

4.3.1.1 Os requisitos operacionais estabelecidos pela AC SAFEWEB CD para a emissão de certificado e para a notificação da emissão à entidade solicitante, estão descritos no item correspondente e sua DPC.

4.3.1.2 Certificados do tipo A1 são considerados válidos a partir do momento de sua emissão; certificados do tipo A3 são considerados válidos a partir da data de início de validade nele constante.

4.3.2 NOTIFICAÇÕES PARA O TITULAR DO CERTIFICADO PELA AC SAFEWEB CD NA EMISSÃO DO CERTIFICADO

O processo utilizado para a notificação de emissão de certificados emitidos pela AC SAFEWEB CD é realizado conforme descrito no item 4.3.1 da sua DPC.

4.4 ACEITAÇÃO DO CERTIFICADO

4.4.1 CONDUTA SOBRE A ACEITAÇÃO DO CERTIFICADO

4.4.1.1 Os requisitos e procedimentos operacionais referentes à aceitação de um certificado por seu titular, estão descritos no item correspondente da DPC da AC SAFEWEB CD.

4.4.1.2 As implicações decorrentes da aceitação ou não aceitação de certificados emitidos pela AC SAFEWEB CD, estão descritas no item correspondente de sua DPC.

4.4.1.3 Termos de acordo, contratos ou instrumentos similares, estão descritos no item 9.16 da PC correspondente, quando aplicável.

4.4.2 PUBLICAÇÃO DO CERTIFICADO PELA AC SAFEWEB CD

O certificado da AC SAFEWEB CD é publicado de acordo com item 2.2 da sua DPC.

4.4.3 NOTIFICAÇÃO DE EMISSÃO DO CERTIFICADO PELA AC RAIZ PARA OUTRAS ENTIDADES

A notificação se dará de acordo com item 2.2 da DPC da AC Raiz.

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

A **AR ARALINK CERTIFICAÇÃO DIGITAL** opera de acordo com a sua própria DPN e com a DPC e PC implementadas pela AC SAFEWEB CD, estabelecidas em conformidade com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1 USABILIDADE DA CHAVE PRIVADA E DO CERTIFICADO DO TITULAR

4.5.1.1 A **AR ARALINK CERTIFICAÇÃO DIGITAL** utiliza sua chave privada e garante a proteção dessa chave conforme o previsto nesta DPN.

4.5.1.2 Obrigações do Titular do Certificado

As obrigações dos titulares de certificados cujas solicitações de emissão são recebidas, validadas e encaminhadas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, constantes dos termos de titularidade de que trata o item 4.1, são as seguintes:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;

d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e

e) informar à **AR ARALINK CERTIFICAÇÃO DIGITAL** ou AC SAFEWEB CD qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Nota: Em se tratando de certificado emitido para pessoa jurídica, estas obrigações se aplicam ao responsável pelo uso do certificado.

4.5.2 USABILIDADE DA CHAVE PÚBLICA E DO CERTIFICADO DAS PARTES CONFIÁVEIS

Em acordo com o item 9.6.4 da DPC da AC SAFEWEB CD.

4.6. RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPN.

4.6.1 CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPN. Exceto para primeira emissão realizada por videoconferência, conforme determina a Resolução n° 170, de 23/04/2020.

4.6.2 QUEM PODE SOLICITAR A RENOVAÇÃO

Em acordo com item 3.3 desta DPN.

4.6.3 PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPN.

4.6.4 NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR

Em acordo com item 3.3 desta DPN.

4.6.5 CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO

Em acordo com item 3.3 desta DPN.

4.6.6 PUBLICAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO PELA AC SAFEWEB CD

Não se aplica.

4.6.7 NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO PELA AC SAFEWEB CD PARA OUTRAS ENTIDADES

Em acordo com item 4.3 da DPC da AC SAFEWEB CD.

4.7 NOVA CHAVE DE CERTIFICADO (RE-KEY)

Não se aplica.

4.8 MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1 CIRCUNSTÂNCIAS PARA REVOGAÇÃO

4.9.1.1 As circunstâncias nas quais um certificado emitido pela AC SAFEWEB CD poderá ser revogado, estão descritas no item correspondente de sua DPC.

4.9.1.2 Um certificado emitido pela AC SAFEWEB CD é obrigatoriamente revogado nas seguintes circunstâncias:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;

b) Quando for necessária a alteração de qualquer informação constante no mesmo;

c) No caso de dissolução da AC SAFEWEB CD;

d) No caso de perda, roubo, acesso indevido, comprometimento da chave privada correspondente ou da sua mídia armazenadora;

e) No caso de falecimento do titular pessoas físicas ou demissão do responsável pela pessoa jurídicas;

f) No caso de mudança na razão ou denominação social do titular da pessoa jurídica;

g) No caso de extinção, dissolução ou transformação do titular do certificado de pessoa jurídica;

h) Por decisão judicial.

4.9.1.3 Deve-se observar ainda que:

a) A AC SAFEWEB CD revogará, no prazo definido no item 4.9.3.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil;

b) O CG da ICP-Brasil, a AC Raiz ou a AC RFB, determinarão a revogação do certificado da AC SAFEWEB CD caso esta deixe de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

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

4.9.1.4.1 Não se aplica.

4.9.1.4.2 Não se aplica.

4.9.1.5 A autenticidade da LCR é confirmada por meio das verificações da assinatura da AC SAFEWEB CD e do período de validade da LCR.

4.9.2 QUEM PODE SOLICITAR A REVOGAÇÃO

A revogação de um certificado, cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, somente pode ser feita:

a) Por solicitação do titular do certificado;

b) Por solicitação do responsável pelo certificado, no caso de certificado de pessoas jurídicas;

c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;

d) Por determinação da AC SAFEWEB CD;

e) Por solicitação da **AR ARALINK CERTIFICAÇÃO DIGITAL** ;

f) Por determinação do CG da ICP-Brasil ou da AC Raiz e da AC RFB;

g) Não se aplica;

h) Não se aplica;

i) Não se aplica.

4.9.3 PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.9.3.1 Para solicitar a revogação é necessário o envio à **AR ARALINK CERTIFICAÇÃO DIGITAL** de um formulário disponibilizado pela AC SAFEWEB CD no site www.safeweb.com.br, preenchido com qualificações do titular ou responsável pelo certificado, tais como: nome completo, CPF, RG, protocolo, tipo do certificado e a indicação do motivo da solicitação. Em caso de pessoa jurídica, indicar também as qualificações da empresa, tais como: razão social, CNPJ, IE, representante legal, CPF e RG, permitindo a identificação inequívoca do solicitante. A AC SAFEWEB CD garante que todos agentes habilitados podem,

facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados conforme o item 4.9.2.

4.9.3.1.1 A confirmação da identidade do solicitante é feita com base na confrontação de dados entre a solicitação de revogação e a solicitação de emissão.

4.9.3.2 Como diretrizes gerais:

a) O solicitante da revogação de um certificado é identificado;

b) As solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas pela AC SAFEWEB CD;

c) As justificativas para a revogação de um certificado são documentadas;

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

4.9.3.3 O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 12 (doze) horas.

4.9.3.4 Não se aplica.

4.9.3.5 A AC SAFEWEB CD responde plenamente por todos os danos causados pelo uso de um 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 desta DPN. O prazo máximo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pela AC SAFEWEB CD é de 3 (três) dias.

4.9.4.2 Não se aplica.

4.9.5 TEMPO EM QUE A AC SAFEWEB CD DEVE PROCESSAR O PEDIDO DE REVOGAÇÃO

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC SAFEWEB CD 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 identificados em cada certificado na cadeia de certificação.

4.9.7 FREQUÊNCIA DE EMISSÃO DE LCR

4.9.7.1 A frequência de emissão da LCR da AC SAFEWEB CD referente a certificados de usuários finais é de 1 (uma) hora.

4.9.7.2 A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 (seis) horas.

4.9.7.3 Não se aplica.

4.9.7.4 Não se aplica.

4.9.7.5 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*

O processo de revogação *on-line* está disponível ao titular do certificado, conforme descrito no item 4.4.3 desta DPN.

4.9.10 REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO *ON-LINE*

Não se aplica.

4.9.11 OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

Não se aplica.

4.9.12 REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE

4.9.12.1 Havendo roubo, perda, modificação, acesso indevido ou qualquer forma de comprometimento da chave privada ou de sua mídia, o titular do certificado deve comunicar imediatamente a **AR ARALINK CERTIFICAÇÃO DIGITAL** ou a AC SAFEWEB CD, de maneira escrita, solicitando a revogação de seu certificado.

4.9.12.2 O comprometimento ou suspeita de comprometimento de chave deve ser comunicado à **AR**

ARALINK CERTIFICAÇÃO DIGITAL ou a AC SAFEWEB CD através do formulário específico para tal fim, devidamente assinado, cujo objetivo é manter os procedimentos para resguardar o sigilo da informação.

4.9.13 CIRCUNSTÂNCIAS PARA SUSPENSÃO

Não se aplica.

4.9.14 QUEM PODE SOLICITAR SUSPENSÃO

Não se aplica.

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 SAFEWEB CD fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados, conforme item 4.9.

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 Em caso de extinção da **AR ARALINK CERTIFICAÇÃO DIGITAL** , serão adotados os procedimentos previstos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.11.2 Em qualquer das hipóteses de descredenciamento da **AR ARALINK CERTIFICAÇÃO DIGITAL** ,

inclusive o encerramento de suas atividades, serão obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação, no Diário Oficial da União e em sua página *web*;

b) após a referida publicação, a AC SAFEWEB CD adotará os seguintes procedimentos, mantendo a guarda de toda a documentação comprobatória em seu poder:

b.1) revogar, em até 3 (três) dias úteis, no sistema de certificação, os acessos dos equipamentos de AR e as autorizações dos agentes de registro da **AR ARALINK CERTIFICAÇÃO DIGITAL** ;

b.2) inventariar os certificados emitidos pela **AR ARALINK CERTIFICAÇÃO DIGITAL** no prazo máximo de 40 (quarenta) dias;

b.3) transferir, se for o caso, de forma segura, a documentação dos certificados gerados pela **AR ARALINK CERTIFICAÇÃO DIGITAL** para o local identificado no requerimento de descredenciamento, no prazo máximo de 50 (cinquenta) dias;

b.4) publicar, em sua página *web*, informação sobre o descredenciamento da **AR ARALINK CERTIFICAÇÃO DIGITAL** , em até 5 (cinco) dias;

b.5) disponibilizar relatório descrevendo todos os procedimentos de descredenciamento adotados para avaliação pela auditoria operacional, no prazo máximo de 60 (sessenta) dias; e

b.6) excluir os agentes de registro do Cadastro de Agentes de Registro – CAR.

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

Não se aplica.

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os controles descritos a seguir são implementados pela **AR ARALINK CERTIFICAÇÃO DIGITAL** para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 CONTROLES FÍSICOS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.1 CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES DA AC SAFEWEB CD

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.2 ACESSO FÍSICO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.2.1 NÍVEIS DE ACESSO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.2.2 SISTEMAS FÍSICOS DE DETECÇÃO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.2.3 SISTEMA DE CONTROLE DE ACESSO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.2.4 MECANISMO DE EMERGÊNCIA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.3 ENERGIA E AR-CONDICIONADO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.4 EXPOSIÇÃO À ÁGUA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.5 PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.6 ARMAZENAMENTO DE MÍDIA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.7 DESTRUIÇÃO DE LIXO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.1.8 INSTALAÇÕES DE SEGURANÇA *(BACKUP)* EXTERNAS *(OFF-SITE)* PARA AC

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.2 CONTROLES PROCEDIMENTAIS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.2.1 PERFIS QUALIFICADOS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.2.2 NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.2.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.2.4 FUNÇÕES QUE REQUEREM SEPARAÇÃO DE DEVERES

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.3 CONTROLES DE PESSOAL

Nos itens seguintes desta DPN são descritos os requisitos e procedimentos, implementados pela **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 **AR ARALINK CERTIFICAÇÃO DIGITAL** , encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

a) Os termos e as condições do perfil que ocuparão;

b) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;

c) 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 **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 ICP-BRASIL [8].

5.3.2 PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

5.3.2.1 Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da **AR ARALINK CERTIFICAÇÃO DIGITAL** envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido a:

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.

5.3.2.2 A **AR ARALINK CERTIFICAÇÃO DIGITAL** não define requisitos adicionais para a verificação de antecedentes.

5.3.3 REQUISITOS DE TREINAMENTO

Todo o pessoal da **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 SAFEWEB CD e das **AR ARALINK CERTIFICAÇÃO DIGITAL** ;

b) Sistema de certificação em uso na AC SAFEWEB CD;

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 **AR ARALINK CERTIFICAÇÃO DIGITAL** envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC SAFEWEB CD e da **AR ARALINK CERTIFICAÇÃO DIGITAL** .

5.3.5 FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

A **AR ARALINK CERTIFICAÇÃO DIGITAL** possui pessoal e efetivo de contingência, devidamente treinados, não fazendo uso de rodízio de pessoal.

5.3.6 SANÇÕES PARA AÇÕES NÃO AUTORIZADAS

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da **AR ARALINK CERTIFICAÇÃO DIGITAL** a AC SAFEWEB CD ou a própria **AR ARALINK CERTIFICAÇÃO DIGITAL** suspenderá o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2 O processo administrativo referido acima contém 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 SAFEWEB CD encaminha suas conclusões à AC RFB e a AC Raiz.

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

a) Advertência;

b) Suspensão por prazo determinado; ou

c) Impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

Todo o pessoal **AR ARALINK CERTIFICAÇÃO DIGITAL** envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.8 DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.3.8.1 A AC SAFEWEB CD torna disponível para todo o seu pessoal e para o pessoal da **AR ARALINK CERTIFICAÇÃO DIGITAL** :

a) A sua Declaração de Práticas de Certificação (DPC);

b) As Políticas de Certificado (PC) que implementa;

c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];

d) Documentação operacional relativa às suas atividades; e

e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2 Toda a documentação fornecida ao pessoal é classificada segundo a política de classificação de informação definida pela AC SAFEWEB CD e é mantida atualizada.

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.2 FREQUÊNCIA DE AUDITORIA DE REGISTROS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.3 PERÍODO DE RETENÇÃO PARA REGISTROS DE AUDITORIA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.4 PROTEÇÃO DE REGISTROS DE AUDITORIA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.5 PROCEDIMENTO PARA CÓPIA DE SEGURANÇA *(BACKUP)* DE REGISTRO DE AUDITORIA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.6 SISTEMA DE COLETA DE DADOS DE AUDITORIA (INTERNO OU EXTERNO)

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.7 NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.4.8 AVALIAÇÕES DE VULNERABILIDADE

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.5 ARQUIVAMENTO DE REGISTROS

5.5.1 TIPOS DE EVENTOS REGISTRADOS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.5.2 PERÍODO DE RETENÇÃO PARA ARQUIVO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.5.3 PROTEÇÃO DE ARQUIVO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.5.4 PROCEDIMENTOS DE CÓPIA DE ARQUIVO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.5.5 REQUISITOS PARA DATAÇÃO DE REGISTROS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.5.6 SISTEMA DE COLETA DE DADOS DE ARQUIVO (INTERNO E EXTERNO)

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.5.7 PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO

A verificação de informação de arquivo deve ser solicitada formalmente à **AR ARALINK CERTIFICAÇÃO DIGITAL** , identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

5.6 TROCA DE CHAVE

5.6.1 Trinta dias antes da data de expiração do certificado digital, a **AR ARALINK CERTIFICAÇÃO DIGITAL** comunica ao seu titular, através do e-mail cadastrado no formulário de solicitação de certificado, a data de expiração do certificado, junto com link para a solicitação de novo certificado.

5.6.2 Não se aplica.

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.7.1 PROCEDIMENTOS GERENCIAMENTO DE INCIDENTE E COMPROMETIMENTO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.7.2 RECURSOS COMPUTACIONAIS, SOFTWARE E/OU DADOS CORROMPIDOS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.7.3 PROCEDIMENTOS NO CASO DE COMPROMETIMENTO DE CHAVE PRIVADA DE ENTIDADE

5.7.3.1 Certificado de entidade é revogado

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.7.3.2 Chave de entidade é comprometida

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.7.4 CAPACIDADE DE CONTINUIDADE DE NEGÓCIO APÓS DESASTRE

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

5.8 EXTINÇÃO DA AC

Em caso de extinção da AC SAFEWEB CD, serão adotados os procedimentos previstos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

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 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.1.1.2 Pares de chaves são gerados somente pelo titular do certificado correspondente. Os procedimentos específicos estão descritos em cada PC implementada pela AC SAFEWEB CD.

6.1.1.3 Cada PC implementada pela AC SAFEWEB CD define o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.1.4 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.1.1.5 Cada PC implementada pela AC SAFEWEB CD caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares de certificados, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.1.6 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR

Item não aplicável, pois a geração e guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

6.1.3.1 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.1.3.2 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*. Os procedimentos específicos aplicáveis são detalhados em cada PC implementada.

6.1.4 ENTREGA DE CHAVE PÚBLICA DA AC ÀS TERCEIRAS PARTES

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.1.5 TAMANHOS DE CHAVE

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

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

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

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

6.1.7.1 Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK**

CERTIFICAÇÃO DIGITAL à AC SAFEWEB CD, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC implementada.

6.1.7.2 Os pares de chaves correspondentes aos certificados cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, 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 pela AC SAFEWEB CD têm ativados os bits *digitalSignature, nonRepudiation e keyEncipherment*.

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

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.1 PADRÕES PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.1.2 O módulo criptográfico utilizado na geração e utilização de chaves criptográficas de titulares de certificados cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, possui certificação INMETRO. Cada PC implementada especifica os requisitos aplicáveis à geração de chaves criptográficas dos titulares de certificado.

6.2.2 CONTROLE "N DE M" PARA CHAVE PRIVADA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.3 RECUPERAÇÃO *(ESCROW)* DE CHAVE PRIVADA

6.2.3.1 O agente de custódia (*escrow*) dos certificados cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, é o PSC Safeweb. Neste caso, 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 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.4 CÓPIA DE SEGURANÇA *(BACKUP)* DE CHAVE PRIVADA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.6 INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.7 ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Ver item 6.1.

6.2.8 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.9 MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.2.10 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas da AC SAFEWEB CD e dos titulares de certificados de assinatura digital e LCR por ela emitidos permanecem armazenadas permanentemente, mesmo após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu período de validade.

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

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.4 DADOS DE ATIVAÇÃO

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

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 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.5.1.2 Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, 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.

6.5.1.2.1 Os requisitos específicos aplicáveis devem ser descritos em cada PC implementada.

6.5.1.3 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.5.1.4 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.5.1.5 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.5.1.6 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.5.2 CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL

Não se aplica.

6.5.3 CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO

6.5.3.1 A **AR ARALINK CERTIFICAÇÃO DIGITAL** implementa requisitos de segurança computacional nas estações de trabalho e computadores portáteis utilizados para os processos de validação e aprovação de certificados.

6.5.3.2 São incluídos os seguintes requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

6.5.3.2.1 A(s) partição(ões) dos discos rígidos das estações de trabalho da **AR ARALINK CERTIFICAÇÃO DIGITAL** que contém componentes da aplicação da AC/AR ou que armazenem dados de solicitantes de certificados digitais são criptografadas.

6.5.3.2.2 As estações de trabalho da **AR ARALINK CERTIFICAÇÃO DIGITAL** implementam aplicação que faz o controle de integridade das configurações da aplicação de AR, bem como dos arquivos de configuração ou informações críticas mantidas na estação de trabalho.

6.5.3.2.3 As estações de trabalho da **AR ARALINK CERTIFICAÇÃO DIGITAL** contém apenas aplicações e serviços que são suficientes e necessários para as atividades corporativas.

6.5.3.2.4 As estações de trabalho da **AR ARALINK CERTIFICAÇÃO DIGITAL** , incluindo equipamentos portáteis, estão protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos e recebem as seguintes configurações de segurança:

a) Controle de acesso lógico ao sistema operacional;

b) Diretivas de senha e de bloqueio de conta;

c) *Logs* de auditoria do sistema operacional ativados, registrando:

I – Iniciação e desligamento do sistema;

II – Tentativas de criar, remover, definir senhas ou mudar privilégios de usuários;

III – Mudanças na configuração da estação;

IV – Tentativas de acesso *(login)* e de saída do sistema *(logoff);*

V – Tentativas não-autorizadas de acesso aos arquivos de sistema;

VI – Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.

d) Antivírus*, antitrojan* e *antispyware*, instalados, atualizados e habilitados.

e) *Firewall* pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por *firewall* corporativo, para equipamentos instalados em redes

que possuam esse dispositivo;

f) Proteção de tela acionada no máximo após 02 (dois) minutos de inatividade;

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

h) Utilização apenas de *softwares* licenciados e necessários para a realização das atividades do agente de registro;

i) Impedimento de *login* remoto, via outro equipamento ligado à rede de computadores utilizada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** , exceto para as atividades de suporte remoto;

j) Utilização de data e hora sincronizadas com a AC Raiz;

k) Equipamentos de coleta biométrica, em atendimento aos padrões da ICP-Brasil;

l) Equipamentos que exijam a identificação biométrica do agente de registro durante a identificação biométrica do requerente do certificado;

6.5.3.2.5 Os *logs* de auditoria do sistema operacional registram os acessos aos equipamentos e ficam armazenados localmente para avaliação pela auditoria operacional ou equipe de segurança.

6.5.3.2.6 A análise desses *logs* somente é realizada em caso de suspeitas quanto a acessos não autorizados ou para dirimir outros tipos de dúvidas que possam surgir sobre a utilização dos equipamentos.

6.5.3.2.7 O agente de registro não possui perfil de administrador ou senha de *root* dos equipamentos ou com privilégios especiais do sistema, ficando essa tarefa delegada a outros da própria organização, para permitir segregação de funções. O agente de registro recebe acesso somente aos serviços e aplicações que tenham sido especificamente autorizados a usar.

6.5.3.2.8 O aplicativo que faz interface entre a **AR ARALINK CERTIFICAÇÃO DIGITAL** e o sistema de certificação da AC SAFEWEB CD possui as seguintes características de segurança:

a) Acesso permitido somente mediante autenticação por meio do certificado do tipo A3 de agente de registro, formalmente autorizado por autoridade competente para ser cadastrado no sistema da AC SAFEWEB CD;

b) Acesso permitido somente a partir de equipamentos autenticados no sistema usando uma identificação única gerada automaticamente a partir de informações do próprio equipamento, o que permite identificá-lo de forma unívoca;

c) *Timeout* de sessão de acordo com a análise de risco da AC;

d) Registro em *log* de auditoria dos eventos citados no item 5.4.1 do DOC-ICP-05 [5];

e) Histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas;

f) Mecanismo para revogação automática dos certificados digitais.

6.5.3.2.9 O aplicativo da Autoridade de Registro:

a) Foi desenvolvido com documentação formal;

b) Possui mecanismos para controle de versões;

c) Possui documentação dos testes realizados em cada versão;

d) Possui documentação comprovando a homologação de cada versão em ambiente com as mesmas características do que será usado em produção, sendo esses ambientes, porém, obrigatoriamente apartados entre si;

e) Possui aprovação documentada do gerente da AC SAFEWEB CD, ou responsável designado, para colocar cada versão em ambiente de produção.

6.5.3.2.10 Os *logs* gerados por esse aplicativo são armazenados na AC SAFEWEB CD pelo prazo de 7 (sete) anos.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

Nos itens seguintes são descritos os controles implementados pela **AR ARALINK CERTIFICAÇÃO DIGITAL** no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 CONTROLES DE DESENVOLVIMENTO DE SISTEMA

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.6.2.1 A **AR ARALINK CERTIFICAÇÃO DIGITAL** verifica a configuração de segurança dos seus sistemas periodicamente, utilizando ferramentas específicas para este fim ou disponibilizadas nativamente pelo sistema operacional. Os dados coletados durante a verificação periódica são comparados com as configurações aprovadas. Caso haja divergência, são tomadas medidas adequadas para a recuperação da situação, levando-se em consideração a natureza do problema e a análise do fato gerador, para evitar a sua recorrência.

6.6.2.2 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.6.3 CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA

Não se aplica.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 DIRETRIZES GERAIS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.7.2 FIREWALL

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.7.3 SISTEMA DE DETECÇÃO DE INTRUSÃO – IDS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.7.4 REGISTRO DE ACESSOS NÃO AUTORIZADOS À REDE

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

6.8 CARIMBO DO TEMPO

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 PERFIL DO CERTIFICADO

Todos os certificados cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD, 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 cuja solicitação de emissão foi recebida, validada e encaminhada pela **AR ARALINK CERTIFICAÇÃO DIGITAL** à AC SAFEWEB CD implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 EXTENSÕES DE CERTIFICADO

Não se aplica.

7.1.3 IDENTIFICADORES DE ALGORITMO

Não se aplica.

7.1.4 FORMATOS DE NOME

Não se aplica.

7.1.5 RESTRIÇÕES DE NOME

Não se aplica.

7.1.6 OID *(OBJECT IDENTIFIER)* DA DPN

Não se aplica.

7.1.7 USO DA EXTENSÃO *"POLICY CONSTRAINTS"*

Não se aplica.

7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Não se aplica.

7.1.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

7.2 PERFIL DE LCR

7.2.1 NÚMERO(s) DE VERSÃO

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

7.2.2 EXTENSÕES DE LCR E DE SUAS ENTRADAS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

7.3 PERFIL DE OCSP

7.3.1 NÚMERO(s) DE VERSÃO

Não se aplica.

7.3.2 EXTENSÕES DE OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

A **AR ARALINK CERTIFICAÇÃO DIGITAL** , bem como as demais entidades integrantes da ICP-Brasil sofre 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 **AR ARALINK CERTIFICAÇÃO DIGITAL** , bem como 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 [2].

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 [3].

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

As auditorias da **AR ARALINK CERTIFICAÇÃO DIGITAL** , bem como 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 [3].

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 da **AR ARALINK CERTIFICAÇÃO DIGITAL** , bem como das entidades

integrantes da ICP-Brasil estão em conformidade com suas respectivas DPCs, PCs, PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust*.

8.4.2 A AC SAFEWEB CD 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 [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3 A **AR ARALINK CERTIFICAÇÃO DIGITAL** também recebeu auditoria prévia para fins de credenciamento. A AC SAFEWEB CD é responsável pela realização de auditorias anuais na **AR ARALINK CERTIFICAÇÃO DIGITAL** , para fins de manutenção de credenciamento, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.5 AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

A **AR ARALINK CERTIFICAÇÃO DIGITAL** cumpre, no prazo estipulado no relatório de auditoria, as recomendações para corrigir as deficiências apontadas indo ao encontro da legislação, políticas, normas, práticas e regras estabelecidas, de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.6 COMUNICAÇÃO DOS RESULTADOS

Os resultados das regularizações são comunicados formalmente à AC RFB, na data de vencimento do prazo concedido no relatório de auditoria de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 TARIFAS

9.1.1 TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS

Variável conforme definição interna comercial.

9.1.2 TARIFA DE ACESSO AO CERTIFICADO

Não são cobradas tarifas de acesso ao certificado digital emitido.

9.1.3 TARIFA DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS

Não há tarifa de revogação.

9.1.4 TARIFA PARA OUTROS SERVIÇOS

Não são cobradas tarifas de acesso à LCR, bem como tarifas de revogação e de acesso aos certificados emitidos.

9.1.5 POLÍTICA DE REEMBOLSO

Não se aplica.

9.2 RESPONSABILIDADE FINANCEIRA

A responsabilidade da **AR ARALINK CERTIFICAÇÃO DIGITAL** será verificada conforme previsto na legislação brasileira.

9.2.1 COBERTURA DE SEGURO

Não se aplica.

9.2.2 OUTROS ATIVOS

Não se aplica.

9.2.3 COBERTURA DE SEGUROS OU GARANTIA PARA ENTIDADES FINAIS

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

9.3.1.1 Como princípio geral, todo documento, informação ou registro fornecido à **AR ARALINK CERTIFICAÇÃO DIGITAL** é sigiloso.

9.3.1.2 Como princípio geral, nenhum documento, informação ou registro fornecido à **AR ARALINK CERTIFICAÇÃO DIGITAL** será divulgado.

9.3.2 INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

Os tipos de informações consideradas não sigilosas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** , compreendem, entre outros:

a) Os certificados e as LCRs emitidos pela AC SAFEWEB CD;

b) Informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;

c) As PCs implementadas pela AC SAFEWEB CD;

d) A DPC da AC SAFEWEB CD;

e) Versões públicas de PS da AC SAFEWEB CD; e

f) A conclusão dos relatórios de auditoria;

g) Política de Garantia;

h) Política de Privacidade; e

i) Declaração de Práticas de Negócio da **AR ARALINK CERTIFICAÇÃO DIGITAL** .

9.3.2.1 Certificados, LCR 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 **AR ARALINK CERTIFICAÇÃO DIGITAL** também são considerados documentos não confidenciais:

a) qualquer DPN;

c) versões públicas de Política de Segurança (PS); e

d) a conclusão dos relatórios da auditoria.

9.3.2.3 A **AR ARALINK CERTIFICAÇÃO DIGITAL** poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados 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 Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.3.3.3 Os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

9.3.3.4 Não se aplica.

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1 PLANO DE PRIVACIDADE

A **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 **AR ARALINK CERTIFICAÇÃO DIGITAL** é 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 são fornecidas na LCR da AC SAFEWEB CD.

9.4.4 RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADA

A **AR ARALINK CERTIFICAÇÃO DIGITAL** é responsável pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS

9.4.5.1 As informações privadas obtidas pela **AR ARALINK CERTIFICAÇÃO DIGITAL** poderão ser utilizadas ou divulgadas a terceiros, mediante expressa autorização do respectivo titular, conforme legislação aplicável.

9.4.5.2 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.

9.4.5.3 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

9.4.6.1 Como diretriz geral, nenhum documento, informação ou registro sob a guarda da **AR ARALINK**

CERTIFICAÇÃO DIGITAL 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.

9.4.6.2 As informações privadas ou confidenciais sob a guarda da **AR ARALINK CERTIFICAÇÃO DIGITAL** 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

Nenhum documento, informação ou registro sob a guarda da **AR ARALINK CERTIFICAÇÃO DIGITAL** é 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 DIREITO DE PROPRIEDADE INTELECTUAL

De acordo com a legislação vigente.

9.6 DECLARAÇÕES E GARANTIAS

9.6.1 DECLARAÇÕES E GARANTIAS DA AC SAFEWEB CD

9.6.1.1 Autorização para certificado

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.6.1.2 Precisão da informação

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.6.1.3 Identificação do requerente

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.6.1.4 Consentimento dos titulares

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.6.1.5 Serviço

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.6.1.6 Revogação

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.6.1.7 Existência Legal

Esta DPN 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 ARALINK CERTIFICAÇÃO DIGITAL

Em acordo com item 4 desta DPN.

9.6.3 DECLARAÇÕES E GARANTIAS DO TITULAR

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

9.6.4 DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES

Conforme descrito no item correspondente da DPC da AC SAFEWEB CD.

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 **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 DPN entra em vigor a partir da sua publicação e permanecerá válida e eficaz até que venha a ser

revogada ou substituída, expressa ou tacitamente.

9.10.2 TÉRMINO

Esta DPN 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 DPN 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 DPN 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 DPN não precisará ser submetida à AC RFB à AC Raiz.

9.12.2 MECANISMO DE NOTIFICAÇÃO E PERÍODOS

Mudança nesta DPC será publicado no site da **AR ARALINK CERTIFICAÇÃO DIGITAL** .

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 DPN serão solucionados de acordo com a legislação vigente.

9.13.2 A DPN da **AR ARALINK CERTIFICAÇÃO DIGITAL** não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14 LEI APLICÁVEL

Esta DPN 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 **AR ARALINK CERTIFICAÇÃO DIGITAL** 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 DPN representa as obrigações e deveres aplicáveis à **AR ARALINK CERTIFICAÇÃO DIGITAL** . Havendo conflito entre esta DPN e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2 CESSÃO

Os direitos e obrigações previstos nesta DPN 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 DPN 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 DPN 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 RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-BRASIL

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

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[13]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

10.2 INSTRUÇÕES NORMATIVAS DA AC RAIZ

Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio https://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	DOC-ICP-05.02
[11]	REGULAMENTO DO USO DE BIOMETRIA NO ÂMBITO DA ICP-BRASIL – SISTEMA BIOMÉTRICO DA ICP-BRASIL	DOC-ICP-05.03

10.3 APROVAÇÕES DA AC RAIZ

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

Ref.	Nome do documento	Código

[4]	TERMOS DE TITULARIDADE	ADE-ICP-05. B

10.4 APROVAÇÕES DA AC RFB

Os documentos abaixo são aprovados pela AC RFB, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.receita.fazenda.gov.br/acrfb/.

Ref.	Nome do documento	Código
[14]	LEIAUTE DOS CERTIFICADOS DIGITAIS DA SECRETARIA DA RECEITA FEDERAL DO BRASIL	VERSÃO 4.4

11 REFERÊNCIAS BIBLIOGRÁFICAS

[15] *Webtrust Principles and Criteria for Registration Authorities*, disponível em https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/webtrust-principles-and-criteria-for-registration-authorities-v10.pdf?la=en&hash=0D5059D7B9D36C1EA3814B50302B66696B62FE82

[16] *Webtrust Principles and Criteria for Certification Authorities,* disponível em: https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/webtrust-for-ca-22.pdf?la=en&hash=F377F94E2E3D87A83D07DDAC54171AC01AE798FA.