

DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS
DA
AR SYSTEM CERTIFICADORA DIGITAL

vinculada à AC SAFEWEB CD

DPN – AR SYSTEM CERTIFICADORA DIGITAL

Versão 1.0

SETEMBRO/2024

Sumário

1	INTRODUÇÃO	5
1.1	VISÃO GERAL.....	5
1.2	NOME DO DOCUMENTO E IDENTIFICAÇÃO.....	5
1.3	PARTICIPANTES DA ICP-BRASIL.....	6
1.4	USABILIDADE DO CERTIFICADO	7
1.5	POLÍTICA DE ADMINISTRAÇÃO	8
1.6	DEFINIÇÕES E ACRÔNIMOS	8
2	RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	10
2.1	REPOSITÓRIOS	10
2.2	PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS.....	11
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.....	13
3.3	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES.....	20
3.4	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO	21
4	REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	21
4.1	SOLICITAÇÃO DE CERTIFICADO	21
4.2	PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO	24
4.3	EMISSÃO DE CERTIFICADO	25
4.4	ACEITAÇÃO DO CERTIFICADO	25
4.5	USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO	26
4.6	RENOVAÇÃO DE CERTIFICADOS.....	26
4.7	NOVA CHAVE DE CERTIFICADO (RE-KEY)	27
4.8	MODIFICAÇÃO DE CERTIFICADO.....	27

AR SYSTEM CERTIFICADORA DIGITAL
DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS – DPN

Vinculada à AC Safeweb CD

Edição: 05.09.2024 | Versão: 1.0

4.9	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	28
4.10	SERVIÇOS DE STATUS DE CERTIFICADO.....	32
4.11	ENCERRAMENTO DE ATIVIDADES	32
4.12	CUSTÓDIA E RECUPERAÇÃO DE CHAVE	33
5	CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL.....	33
5.1	CONTROLES FÍSICOS.....	33
5.2	CONTROLES PROCEDIMENTAIS.....	34
5.3	CONTROLES DE PESSOAL	35
5.4	PROCEDIMENTOS DE LOG DE AUDITORIA	38
5.5	ARQUIVAMENTO DE REGISTROS.....	39
5.6	TROCA DE CHAVE.....	39
5.7	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	40
5.8	EXTINÇÃO DA AC.....	40
6	CONTROLES TÉCNICOS DE SEGURANÇA.....	40
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	40
6.2	PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO	42
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	43
6.4	DADOS DE ATIVAÇÃO	44
6.5	CONTROLES DE SEGURANÇA COMPUTACIONAL	44
6.6	CONTROLES TÉCNICOS DO CICLO DE VIDA	47
6.7	CONTROLES DE SEGURANÇA DE REDE	48
6.8	CARIMBO DO TEMPO	48
7	PERFIS DE CERTIFICADO, LCR E OCSP	49
7.1	PERFIL DO CERTIFICADO	49
7.2	PERFIL DE LCR	50
7.3	PERFIL DE OCSP.....	50
8	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	50
8.1	FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES.....	50
8.2	IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR	50
8.3	RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA.....	51
8.4	TÓPICOS COBERTOS PELA AVALIAÇÃO.....	51

AR SYSTEM CERTIFICADORA DIGITAL
DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS – DPN

Vinculada à AC Safeweb CD

Edição: 05.09.2024 | Versão: 1.0

8.5	AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA.....	51
8.6	COMUNICAÇÃO DOS RESULTADOS.....	52
9	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	52
9.1	TARIFAS	52
9.2	RESPONSABILIDADE FINANCEIRA	52
9.3	CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO	53
9.4	PRIVACIDADE DA INFORMAÇÃO PESSOAL.....	54
9.5	DIREITO DE PROPRIEDADE INTELECTUAL	55
9.6	DECLARAÇÕES E GARANTIAS	56
9.7	ISENÇÃO DE GARANTIAS.....	57
9.8	LIMITAÇÕES DE RESPONSABILIDADES	57
9.9	INDENIZAÇÕES.....	57
9.10	PRAZO E RESCISÃO.....	57
9.11	AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES	57
9.12	ALTERAÇÕES.....	58
9.13	SOLUÇÃO DE CONFLITOS	58
9.14	LEI APLICÁVEL	58
9.15	CONFORMIDADE COM A LEI APLICÁVEL.....	58
9.16	DISPOSIÇÕES DIVERSAS	58
9.17	OUTRAS PROVISÕES	59
10	DOCUMENTOS REFERENCIADOS.....	59
10.1	RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-BRASIL.....	59
	DOC-ICP-09.....	59
	DOC-ICP-08.....	59
	DOC-ICP-05.....	59
	DOC-ICP-03.....	59
	DOC-ICP-04.....	59
	DOC-ICP-02.....	59
	DOC-ICP-06.....	59
10.2	INSTRUÇÕES NORMATIVAS DA AC RAIZ.....	60
10.3	APROVAÇÕES DA AC RAIZ	60

Rua Elzir Matos, nº s/n, Centro, Piancó/PB - CEP: 58.765-000

PIANCÓ,PB, Brasil – CEP

30.713.872/0001-68 | <https://systemcertificadora.com/>

10.4 APROVAÇÕES DA AC RFB 60
11 REFERÊNCIAS BIBLIOGRÁFICAS 60

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	05/09/2024	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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA DIGITAL**”, referido a seguir simplesmente como "DPN – **AR SYSTEM CERTIFICADORA DIGITAL**" e descreve as práticas e os procedimentos empregados pela **AR SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 INAPTA, SUSPENSA, BAIXADA ou NULA conforme o disposto nos incisos I e II do art. 6º da Instrução Normativa RFB nº 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 nos PCs correspondentes.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

“AR»: **AR SYSTEM CERTIFICADORA DIGITAL**

1.5.2 CONTATOS

Endereço:

Telefone:

Página web:

E-mail:

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPN COM A DPC

Nome:

Telefone:

E-mail:

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

AR SYSTEM CERTIFICADORA DIGITAL
DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS – DPN

Vinculada à AC Safeweb CD

Edição: 05.09.2024 | Versão: 1.0

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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 "Distinguished 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 se referem 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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.

AR SYSTEM CERTIFICADORA DIGITAL
DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS – DPN

Vinculada à AC Safeweb CD

Edição: 05.09.2024 | Versão: 1.0

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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA 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 SYSTEM CERTIFICADORA DIGITAL**. Toda referência a formulário deverá ser entendida também como referência a outras formas que a **AR SYSTEM CERTIFICADORA DIGITAL** possa vir a adotar. Dentre os requisitos e procedimentos operacionais estabelecidos pela **AR SYSTEM CERTIFICADORA 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 anexo 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;

AR SYSTEM CERTIFICADORA DIGITAL
DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS – DPN

Vinculada à AC Safeweb CD

Edição: 05.09.2024 | Versão: 1.0

- 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.