DPN – DECLARAÇÕES DE PRÁTICAS DE NEGÓCIOS - AR

AR CÂMARA DE DIRIGENTES LOJISTAS DE PATOS DE MINAS

Versão 2.0 Janeiro/ 2022

Sumário

1. INTRODUÇÃO 6
1.1. VISÃO GERAL 6
1.2. PARTICIPANTES DA ICP-BRASIL 6
1.2.1. AUTORIDADE DE REGISTRO (AR) 6
1.3. TITULARES DE CERTIFICADO 6
1.3.1. PARTES CONFIÁVEIS 7
1.4. USABILIDADE DO CERTIFICADO 7
1.4.1. USO APROPRIADO DO CERTIFICADO 7
1.4.2. USO PROIBITIVO DO CERTIFICADO 7
1.5. POLÍTICA DE ADMINISTRAÇÃO 7
1.5.1. ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO 7
1.5.2. CONTATOS 7
1.5.3. PESSOA QUE DETERMINA A ADEQUABILIDADE DESTA DPN 7
1.5.4. PROCEDIMENTOS DE APROVAÇÃO DA DPN 8
1.6. DEFINIÇÕES E ACRÔNIMOS 8
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 9
2.1. REPOSITÓRIOS 9
2.1.1. OBRIGAÇÕES DAS AR´S 9
2.2. CONTROLES DE ACESSO AOS REPOSITÓRIOS 10
3. IDENTIFICAÇÃO E AUTENTICAÇÃO 10
3.1. ATRIBUIÇÃO DE NOMES 10
3.1.1. TIPOS DE NOMES 10
3.1.2. NECESSIDADE DE NOMES SEREM SIGNIFICATIVOS 10
3.1.3. ANONIMATO OU PSEUDÔNIMO DOS TITULARES DO CERTIFICADO 10
3.1.4. REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES 10
3.1.5. UNICIDADE DE NOMES 10
3.1.6. PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES 11
3.1.7. RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS 11
3.2. VALIDAÇÃO INICIAL DE IDENTIDADE 11
3.2.1. MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA 11

3.2.2. AUTENTICAÇÃO DA IDENTIFICAÇÃO DA ORGANIZAÇÃO 12
3.2.2.1 DISPOSIÇÕES GERAIS 12
3.2.2.2 DOCUMENTOS PARA EFEITO DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO 12
3.2.2.3 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO 13
3.2.3. AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO 13
3.2.3.1 PROCEDIMENTOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO 13
3.2.4. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO 15
3.2.5. INFORMAÇÕES NÃO VERIFICADAS DO TITULAR DO CERTIFICADO 15
3.2.6. PROCEDIMENTOS COMPLEMENTARES 15
3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES 16
3.3.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA ROTINA DE NOVAS CHAVES ANTES DA EXPIRAÇÃO 16
3.3.2. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA NOVAS CHAVES APÓS A REVOGAÇÃO 17
3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO 17
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 17
4.1. SOLICITAÇÃO DE CERTIFICADO 17
4.1.2. PROCESSO DE REGISTRO E RESPONSABILIDADES 18
4.1.3. RESPONSABILIDADES DA AR 18
4.1.4. OBRIGAÇÕES DAS ARS 18
4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO 19
4.2.1. EXECUÇÃO DAS FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO 19
4.2.2. APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO 19
4.2.3. TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO 19
4.3. EMISSÃO DE CERTIFICADO 19
4.3.1. AÇÕES DA AC CNDL RFB DURANTE A EMISSÃO DE UM CERTIFICADO 19
4.3.2. NOTIFICAÇÕES PARA O TITULAR DO CERTIFICADO PELA AC CNDL RFB NA EMISSÃO DO CERTIFICADO 19
4.4. ACEITAÇÃO DO CERTIFICADO 20
4.4.1. CONDUTA SOBRE A ACEITAÇÃO DO CERTIFICADO 20
4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO 20
4.5.1. USABILIDADE DA CHAVE PRIVADA E DO CERTIFICADO DO TITULAR 20
4.6. RENOVAÇÃO DE CERTIFICADOS 21
4.6.1. CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS 21
4.6.2. QUEM PODE SOLICITAR A RENOVAÇÃO 21
4.6.3. PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS 21
4.6.4. NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR 21

4.6.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO .. 21
4.7. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO 21
4.7.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO 21
4.7.2. QUEM PODE SOLICITAR REVOGAÇÃO 22
4.7.3. PROCEDIMENTO PARA SOLICITAR REVOGAÇÃO 22
4.7.4. PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO 23
4.7.5. TEMPO EM QUE A AC CNDL RFB e AR´S VINCULADAS DEVEM PROCESSAR O PEDIDO DE REVOGAÇÃO 23
4.7.6. DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE 23
4.7.7. REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE 23
4.8. CIRCUNSTÂNCIAS PARA SUSPENSÃO 23
4.9. ENCERRAMENTO DE ATIVIDADES 24
5. CONTROLES PROCEDIMENTAIS 24
5.1. PERFIS QUALIFICADOS 24
5.2. NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA 25
5.2.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL 25
5.3. FUNÇÕES QUE REQUEREM SEPARAÇÃO DE DEVERES 25
5.3.1. CONTROLES DE PESSOAL 25
5.3.2. ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE 26
5.3.3. PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES 26
5.3.4. FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA 26
5.3.5. FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS 26
5.3.6. SANÇÕES PARA AÇÕES NÃO AUTORIZADAS 26
5.3.7. REQUISITOS PARA CONTRATAÇÃO DE PESSOAL 27
5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL 27
5.4. TROCA DE CHAVE 27
5.5. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE 27
5.5.1. PROCEDIMENTOS GERENCIAMENTO DE INCIDENTE E COMPROMETIMENTO 27
6. CONTROLES DE SEGURANÇA 28
6.1. CONTROLES DE SEGURANÇA PARA AUTORIDADES DE REGISTRO 28
6.2. CONTROLES TÉCNICOS DO CICLO DE VIDA 30
6.2.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA 30
6.3. CONTROLES DE GERENCIAMENTO DE SEGURANÇA 30
7. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES 30
8. TÓPICOS COBERTOS PELA AVALIAÇÃO 31
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 31

9.1. TARIFAS 31
9.1.1. TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS 31
9.1.2. TARIFA DE ACESSO AO CERTIFICADO 31
9.1.3. TARIFA DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS 31
9.1.4. TARIFA PARA OUTROS SERVIÇOS 31
9.1.5. POLÍTICA DE REEMBOLSO 31
9.2. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO 31
9.2.1. ESCOPO DE INFORMAÇÕES CONFIDENCIAIS 31
9.2.2. INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS 31
9.3. RESPONSABILIDADE EM PROTEGER A INFORMAÇÃO CONFIDENCIAL 32
9.4. PRIVACIDADE DA INFORMAÇÃO PESSOAL 32
9.4.1. PLANO DE PRIVACIDADE 32
9.4.2. TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS 32
9.4.3. RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADA 32
9.4.4. AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS 32
9.4.5. INFORMAÇÕES A TERCEIROS 33
9.5. DECLARAÇÕES E GARANTIAS 33
9.5.1. DECLARAÇÕES E GARANTIAS DA AR 33
9.5.2. DECLARAÇÕES E GARANTIAS DO TITULAR 33
9.6. DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES 33
9.7. PRAZO E RESCISÃO 33
9.7.1. PRAZO 33
9.7.2. TÉRMINO 33
9.7.3. EFEITO DA RESCISÃO E SOBREVIVÊNCIA 33
9.7.4. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES 33
9.8. ALTERAÇÕES 33
9.8.1. MECANISMO DE NOTIFICAÇÃO E PERÍODOS 33
10. PRÁTICAS COMERCIAIS ARV´S 34
10.1. POLÍTICA DE GARANTIA 34
10.2. POLÍTICA DE ARREPENDIMENTO 34
11. DOCUMENTOS REFERENCIADOS 35
11.1. RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-BRASIL 35

Autor: Confederação Nacional de Dirigentes Lojistas - SPC Brasil

Edição: 24/01/2022 **Versão:** 2.0

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1. As informações contidas neste documento estabelecem os requisitos mínimos, obrigatoriamente observados pela Autoridade Certificadora CNDL RFB e AR´S vinculadas. A AC é integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. Esta DPN é o documento que descreve as práticas e os procedimentos empregados pelas AR´S vinculadas na execução de seus serviços.

1.1.2. A elaboração desta DPN foi disciplinada no DOC-ICP-05 do Comitê Gestor da ICP-Brasil que obrigatoriamente adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10] bem como Princípios e Critérios WebTrust para AR [5];

1.1.3. As AR´S vinculadas mantém todas as informações da suas DPN sempre atualizadas.

1.2. PARTICIPANTES DA ICP-BRASIL

1.2.1. AUTORIDADE DE REGISTRO (AR)

1.2.1.1 Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência das Autoridades de Registro (AR).

As Autoridades de Registro vinculadas (AR) à AC CNDL RFB estão relacionadas na página Web https://www.spcbrasil.org.br/certificacaodigital/suporte/duvidas-frequentes que contém as seguintes informações:

a) Relação de todas as AR credenciadas, com informações sobre as PC que implementam;

b) Relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;

1.3. TITULARES DE CERTIFICADO

Podem ser titulares de certificados emitidos AR´S vinculadas, Pessoas físicas inscritas no CPF, desde que não enquadradas na situação cadastral de CANCELADA ou NULA ou jurídicas de direito público ou privado, nacionais ou internacionais, 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. 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).

NOTA 1: Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrada no CNPJ da RFB. Preferencialmente será designado como

responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.1. PARTES CONFIÁVEIS

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

1.4. USABILIDADE DO CERTIFICADO

1.4.1. USO APROPRIADO DO CERTIFICADO

As AR´S Vinculadas praticam as seguintes Políticas de Certificado Digital:

Política de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da AC CNDL RFB	PC AC CNDL RFB A1	2.16.76.1.2.1.52
Política de Certificado de Assinatura Digital tipo A3 da AC CNDL RFB	PC AC CNDL RFB A3	2.16.76.1.2.3.49

Nas PCs correspondentes estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC CNDL RFB.

1.4.2. USO PROIBITIVO DO CERTIFICADO

Quando cabível, as aplicações para as quais existam restrições ou proibições para o uso desses certificados, estão listados nas PC´S implementadas.

1.5. POLÍTICA DE ADMINISTRAÇÃO

1.5.1. ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AR: Câmara de Dirigentes Lojistas de Patos de Minas

1.5.2. CONTATOS

Rua: Dores de Indaiá, 17
CEP: 38700-140
Bairro: Centro Cidade: Patos de Minas Estado: MG
Telefones: (34) 3818-3400
Contato: (34) 3818-3400
E-mail: gerencia@cdlpatosdeminas.org.br
Pág. Web: https://cdlpatosdeminas.org.br

1.5.3. PESSOA QUE DETERMINA A ADEQUABILIDADE DESTA DPN

Nome: Marli Paiva Rubio e Vanessa Danielle Rocha Berloni

Telefone: (11) 3549-6800

E-mail: controlesinternos@spcbrasil.org.br

Outros: Setor de Compliance & Controles Internos da AC CNDL

1.5.4. PROCEDIMENTOS DE APROVAÇÃO DA DPN

Esta DPN é aprovada pela AC. Os procedimentos de aprovação da DPN das AR´S vinculadas são estabelecidos a critério do CG da ICP-Brasil.

1.6. DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
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
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
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
TSC	Tribunal Superior Eleitoral
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. REPOSITÓRIOS

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas.

2.1.1. OBRIGAÇÕES DAS AR´S

As obrigações das AR´S vinculadas em relação ao seu repositório estão abaixo relacionadas:

a) Publicar em sua página web, sua DPN aprovada assim que implementada;

2.2. CONTROLES DE ACESSO AOS REPOSITÓRIOS

Somente a AC CNDL RFB por seus funcionários competentes e designados especialmente para esse fim, poderão alterar as informações constantes nesta DPN.

Não há restrições para o acesso da leitura desta DPN. Todas as informações disponibilizadas pela AR, estão disponíveis para leitura sem restrições.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

As AR´S vinculadas verificam a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os direitos de propriedade intelectual de terceiros. A AR vinculadas reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1. ATRIBUIÇÃO DE NOMES

3.1.1. TIPOS DE NOMES

3.1.1.1. As AR´S vinculadas emitem certificados com nomes que permitam a identificação unívoca. Para isso utiliza o "distinguished name" do padrão ITU X.500, endereços de correio eletrônico ou endereços de página Web (URL). O certificado emitido para pessoa jurídica inclui o nome da pessoa física responsável. Para todos os efeitos legais, os certificados e as respectivas chaves de assinatura são de titularidade do responsável constante do certificado.

3.1.2. NECESSIDADE DE NOMES SEREM SIGNIFICATIVOS

3.1.2.1. As AR´S vinculadas 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 por elas.

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.

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.

3.1.3. ANONIMATO OU PSEUDÔNIMO DOS TITULARES DO CERTIFICADO

Item não aplicável.

3.1.4. REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES

Item não aplicável.

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 CNDL RFB. 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

No âmbito da AC CNDL RFB não há disputa decorrente de igualdade de nomes entre solicitantes de certificados pois o nome do Titular do Certificado será formado a partir do nome constante dos cadastros da RFB, CPF ou CNPJ para certificados de pessoa física ou jurídica respectivamente, acrescido do número de inscrição nestes cadastros. Este procedimento garante a unicidade de todos os nomes no âmbito da AC CNDL RFB.

3.1.7. RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS

Tais procedimentos são analisados com base na legislação em vigor.

3.2. VALIDAÇÃO INICIAL DE IDENTIDADE

As AR´S vinculadas utilizam os seguintes requisitos e procedimentos para realização dos seguintes processos:

a) Identificação 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., 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/ou biometria apresentada, 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 possuí 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.

III – Emissão do certificado: conferência dos dados da solicitação do certificado com os constantes nos documentos e biometrias apresentados na etapa de identificação é liberada a emissão do certificado no sistema da AC CNDL RFB. 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 AC e AR verificam se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. As RFC 4210 e 6712 são utilizadas como referência para essa finalidade.

3.2.2. AUTENTICAÇÃO DA IDENTIFICAÇÃO DA ORGANIZAÇÃO

3.2.2.1 DISPOSIÇÕES GERAIS

Os métodos empregados para confirmação da identidade de pessoa jurídica são feitos mediante consulta as bases de dados da RFB.

Quando se tratar de titular do certificado pessoa jurídica, será designado o representante legal da pessoa jurídica como responsável pelo certificado, que será o detentor da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica.

A confirmação da identidade da organização e das pessoas físicas deverá ser feita nos seguintes termos:

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

b) Apresentação do rol de documentos elencados no item 3.2.3. do responsável pelo uso do certificado; e

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 do termo de titularidade de que trata o item 4.4. pelo titular ou responsável pelo uso do certificado.

3.2.2.2 DOCUMENTOS PARA EFEITO DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

Durante a solicitação de certificado e-CNPJ é realizada consulta à situação cadastral do CNPJ junto ao cadastro da RFB. Se o CNPJ estiver INAPTO, CANCELADO, BAIXADO, NULO ou SUSPENSO – situações que impedem o fornecimento do certificado - a solicitação não é enviada para a AC CNDL RFB. 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, cópia do CNPJ:,

ii. se entidade privada:

1) certidão simplificada emitida pela Junta Comercial ou ato constitutivo (original ou cópia autenticada), 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 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

3.2.5.1. O preenchimento dos seguintes campos do certificado de uma pessoa jurídica, são obrigatórios, com as informações constantes nos documentos apresentados:

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

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);

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

d) Data de nascimento do responsável pelo certificado.

3.2.5.2. Toda PC pode definir a obrigatoriedade do preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá também solicitar o preenchimento de campos do certificado suas informações pessoais.

3.2.3. AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO

Durante a solicitação do certificado modelo e-CPF é realizada consulta da situação cadastral do solicitante perante o CPF, 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 à AC CNDL RFB.

A confirmação da identidade é realizada mediante a presença física do interessado, ou por um dos procedimentos listados nas alíneas abaixo, que, 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;

a) Por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz.

3.2.3.1 PROCEDIMENTOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

Deverá ser apresentada a seguinte documentação, em sua versão original, podendo ser física ou digital, por meio de barramento ou aplicação oficial, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado:

a) Registro de Identidade, se brasileiro;

b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;

c) Passaporte, se estrangeiro não domiciliado no Brasil;

d) Título de eleitor com foto;

e) 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 admitidos 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 emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

NOTA 3: Os documentos que possuem data de validade precisam estar dentro prazo. Excepcionalmente o RG e a CNH, poderão ser aceitas para identificação de titular de certificado digital.

NOTA 4: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a CNH - Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

NOTA 5: 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.

O e-mail de comunicação é obrigatório, e de inteira responsabilidade do titular, e serve 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 poderá dispensada a apresentação de qualquer dos documentos elencados no item 3.2.7. e da 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.

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) pela AR ou AR própria da AC, ou ainda AR própria do PSS; 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.

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.

3.2.4. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

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

a) Cadastro de Pessoa Física (CPF);

b) Nome completo, sem abreviações;

c) Data de nascimento

d) e-mail.

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

a) Cadastro de Pessoa Física (CPF)

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

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

d) Número do Cadastro Especifico do INSS (CEI) ou CAEPF;

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

f) Número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

3.2.4.3. 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.

3.2.5. INFORMAÇÕES NÃO VERIFICADAS DO TITULAR DO CERTIFICADO

Item não aplicável.

3.2.6. PROCEDIMENTOS COMPLEMENTARES

3.2.6.1. A AC CNDL RFB e as AR´S vinculadas mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos Webtrust Principles and Criteria for Certification Authorities [15], disponível no endereço Webtrust CA.

3.2.6.2. Todo o processo de identificação do titular do certificado deve ser registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC CNDL RFB, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. O sistema biométrico da ICP-BRASIL deve solicitar 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

devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.2.6.3. 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 em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR´S da ICP-Brasil.

3.2.6.4. A AC CNDL RFB deve disponibilizar, para todas as AR´S vinculadas a sua respectiva cadeia, 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 CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6] e em regulamento editado por instrução normativa da AC Raiz que defina os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil.

3.2.6.4.1. 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.

3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA ROTINA DE NOVAS CHAVES ANTES DA EXPIRAÇÃO

3.3.1.1. Os métodos de identificação do solicitante utilizados pelas AR´S vinculadas para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente estão estabelecidos no item subsequente.

3.3.1.2. Tal processo será conduzido segundo uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;

b) solicitação por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido do tipo A3 ou superior, que seja pelo menos 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 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 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.

3.3.2. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA NOVAS CHAVES APÓS A REVOGAÇÃO

3.3.2.1. Após a revogação ou expiração do certificado, o solicitante pode requerer um novo certificado, enviando à AC CNDL RFB, ou AR Vinculada uma solicitação, na forma, condições e prazo estabelecidos como a solicitação inicial de um certificado.

3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

3.4.1 A solicitação de revogação de certificado deve permitir a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados entre a solicitação de revogação e a solicitação de emissão, cadastrados na AR.

3.4.2. Os procedimentos para solicitação de revogação de certificado estão descritos no item 4.7 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 AC CNDL é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR Vinculada. Toda referência a formulário deverá ser entendida também como referência a outras formas que a AR Vinculada possa vir a adotar.

Dentre os requisitos e procedimentos operacionais estabelecidos pela AC CNDL RFB para as solicitações de emissão de certificado, estão:

a) a comprovação de atributos de identificação constantes do certificado;

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

c) um termo de titularidade assinado pelo titular do certificado e um termo de responsabilidade assinado pelo responsável pelo uso do certificado, elaborados conforme o documento TERMO DE TITULARIDADE [4].

d) A confirmação de cadastro por videoconferência realizada por agente de registro devidamente habilitado e autorizado, nas situações descritas nos itens 3.2.2. e 3.2.3. As AR´S vinculadas à AC CNDL asseguram que os meios técnicos utilizados são adequados a garantir que a videoconferência pois:
d.1) Preservam a integridade e confidencialidade da comunicação audiovisual entre o AGR e o requerente através da utilização de sessões de vídeo protegidas com criptografia “ponta-a-ponta”;

d.2) Permitem que os AGR´S que apliquem questionários sequenciais (scripts), de forma aleatória ao cliente, de modo que a sequência de perguntas nunca seja a mesma e, portanto, não possa ser prevista, para que o AGR colete informações para atestar a veracidade da identificação da pessoa que se apresenta em vídeo e o seu respectivo cadastro;
d.3) Garantem que o AGR tem real assertividade de que as informações da pessoa jurídica constantes no documento de identificação apresentado correspondem efetivamente à pessoa jurídica requerente a ser identificada;
d.4) Os AGR´S das AR´S vinculadas a AC CNDL RFB, certificam-se sobre a veracidade da informação contida no documento de identificação do requerente, quando um documento de identificação for utilizado.

No caso de pessoa física titular de certificado expirado, previamente identificada e cadastrada presencialmente, e cujos dados biométricos tenham sido devidamente coletados, a geração de novo par de chaves poderá ser realizada mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme requisitos do DOC-ICP 05.05 [16].

No caso de uma organização titular de certificado expirado, cujo responsável pelo certificado seja o mesmo ora solicitando novo certificado, que foi previamente identificado e cadastrado presencialmente, e cujos dados biométricos tenham sido devidamente coletados, a geração de novo par de chaves poderá ser realizada mediante confirmação do respectivo cadastro, da organização e do responsável pelo certificado, por meio de videoconferência, conforme requisitos do DOC-ICP 05.05 [16].

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 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.

4.1.2. 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.

4.1.3. RESPONSABILIDADES DA AR

A AR será responsável pelos danos a que der causa.

4.1.4. OBRIGAÇÕES DAS ARS

Neste item estão contempladas as obrigações das ARs vinculadas à AC CNDL RFB, abaixo relacionadas:

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 responsável utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina as características

mínimas de segurança para as AR´S 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 CNDL RFB e pela ICP-Brasil, em especial com o contido contido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR´S da ICP-Brasil, bem como os Princípios e Critérios *WebTrust* para AR;

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. e 3.2.3; e

h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios *WebTrust* para AR [5].

4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1. EXECUÇÃO DAS FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC CNDL RFB e AR´S executam 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. A AR´S vinculadas podem, 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´S vinculadas 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 CNDL RFB DURANTE A EMISSÃO DE UM CERTIFICADO

Após a validação da solicitação do certificado, de que trata o item 3.2, a AC CNDL RFB procede à emissão do certificado. O certificado emitido é inserido na relação de certificados emitidos pela AC CNDL RFB.

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 CNDL RFB NA EMISSÃO DO CERTIFICADO

Após a emissão do certificado, a AC e AR´S vinculadas é realizada através de e-mail, conforme descrito no item 4.3.1 desta DPC.

4.4. ACEITAÇÃO DO CERTIFICADO

4.4.1. CONDUTA SOBRE A ACEITAÇÃO DO CERTIFICADO

4.4.1.1. O certificado é considerado aceito assim que for utilizado. A aceitação implica que a pessoa física responsável pelo certificado reconhece a veracidade dos dados contidos nele.

4.4.1.2. A aceitação de todo certificado emitido é declarada implicitamente pelo respectivo titular assim que for utilizado. Para certificados emitidos para pessoas jurídicas, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

Ao aceitar um e-CPF, o Titular:

1) Está ciente e de acordo com as responsabilidades, obrigações e deveres impostos pelo Termo de Titularidade, pela PC implementada e por esta DPN;

2) Garante que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

3) Afirma que as informações fornecidas durante o processo de solicitação são verdadeiras e foram publicadas dentro do certificado com exatidão.

Ao aceitar um e-CNPJ, o Titular e o Responsável pelo uso do certificado:

1) Estão cientes e de acordo com as responsabilidades, obrigações e deveres impostos a eles pelo Termo de Titularidade e Responsabilidade, pela PC implementada e por esta DPN;

2) Garantem que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

3) Afirmam que as informações fornecidas durante o processo de solicitação, são verdadeiras e foram publicadas dentro do certificado com exatidão.

4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

A AC CNDL RFB e AR´S vinculadas operam de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementa, estabelecidos em conformidade com este documento e 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 AC CNDL RFB utiliza sua chave privada e garante a proteção dessa chave conforme o previsto na sua própria DPC.

4.5.1.2. Obrigações do Titular do Certificado

Neste item foram incluídas as obrigações dos titulares de certificados emitidos pela AC CNDL RFB e AR´S vinculadas, constantes dos termos de titularidade, abaixo relacionados:

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

b) garantir a proteção e o sigilo de suas chaves privadas, 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, pela PC e DPN correspondente e por outros documentos aplicáveis da ICP-Brasil; e

e) informar à AC CNDL RFB 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.

4.6. RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 4.3.1. desta DPN.

4.6.1. CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 4.3.1. desta DPN.

4.6.2. QUEM PODE SOLICITAR A RENOVAÇÃO

Em acordo com item 4.3.1. desta DPN.

4.6.3. PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 4.3.1. desta DPN.

4.6.4. NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR

Em acordo com item 4.3.1. desta DPN.

4.6.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO

Em acordo com item 4.3.1. desta DPN.

4.7. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.7.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO

4.7.1.1. As AR´S vinculadas, nesta DPN evidenciam as circunstâncias nas quais um certificado poderá ser revogado.

4.7.1.2. Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

a) Caso haja constatação de emissão imprópria ou defeituosa do mesmo;

b) Mediante a necessidade de alteração de qualquer informação constante no mesmo; ou

c) Em caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora.

d) No caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;

e) No caso de falecimento do titular - pessoas físicas;

f) No caso de mudança na razão ou denominação social do titular - pessoas jurídicas;

g) No caso de extinção, dissolução ou transformação do titular do certificado - pessoas jurídicas;

h) No caso de dissolução da AC CNDL RFB;

i) No caso de falecimento ou demissão do responsável - pessoas jurídicas; ou

j) Por decisão judicial.

4.7.1.3. Deve-se observar ainda que:

a) A AR´S vinculadas revogarão, no prazo definido nesta DPN, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil;

b) O CG da ICP-Brasil determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

c) A AC RFB determinará a revogação do certificado da AC CNDL RFB, caso esta deixe de cumprir as normas, práticas e regras estabelecidas pela RFB.

4.7.1.4. Todo certificado tem a sua validade verificada, na respectiva LCR, antes de ser utilizado.

4.7.2. QUEM PODE SOLICITAR REVOGAÇÃO

A revogação de um certificado somente pode ser solicitada:

a) Pelo titular do certificado;

b) Pelo responsável pelo certificado de pessoas jurídicas;

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

d) Pela AC CNDL RFB;

e) Pela AC RFB;

f) Pela AR Vinculada que recebeu a solicitação; ou

g) Por determinação da AC RFB, do CG da ICP-Brasil ou da AC Raiz.

4.7.3. PROCEDIMENTO PARA SOLICITAR REVOGAÇÃO

4.7.3.1. Para requerer a revogação é necessário o envio à AC CNDL RFB ou à AR vinculada de um formulário disponibilizado pela AC CNDL RFB (https://www.spcbrasil.org.br/certificacaodigital/suporte/revogacao), preenchido com os dados do solicitante, 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, representante legal, CPF e RG, permitindo a identificação inequívoca do solicitante. A AC CNDL RFB garante que todos agentes habilitados, conforme o item 4.9.2., possam, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados.

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

4.7.3.2. 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;

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.

4.7.3.3. 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 24 (vinte e quatro) horas.

4.7.3.4. A AC CNDL RFB e AR´S vinculadas respondem 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.

4.7.4. PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.7.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.7.7.

4.7.4.2. 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 CNDL RFB é de 3 (três) dias.

4.7.5. TEMPO EM QUE A AC CNDL RFB e AR´S VINCULADAS DEVEM PROCESSAR O PEDIDO DE REVOGAÇÃO

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC CNDL RFB e AR´S vinculadas devem processar a revogação imediatamente após a análise do pedido.

4.7.6. DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE

O processo de revogação on-line está disponível ao titular do certificado.

4.7.7. REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE

4.7.7.1. 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 AC CNDL RFB ou AR´S vinculadas, de maneira escrita, solicitando a revogação de seu certificado.

4.7.7.2. O comprometimento ou suspeita de comprometimento de chave deve ser comunicado à AC CNDL RFB ou AR´S vinculadas através do formulário específico para tal fim, devidamente assinado, cujo objetivo é manter os procedimentos para resguardar o sigilo da informação.

4.8. CIRCUNSTÂNCIAS PARA SUSPENSÃO

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

4.9. ENCERRAMENTO DE ATIVIDADES

4.9.1. Em caso de extinção da AC CNDL RFB e AR´S vinculadas, serão adotados os procedimentos previstos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.9.2. Quando for necessário encerrar as atividades da AC CNDL RFB ou da AR vinculada, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes, inclusive:

a) Notificar a AC Raiz da ICP-Brasil;

b) Extinguir a emissão, revogação e publicação de LCR e/ou dos serviços de status on-line, após a revogação de todos os certificados emitidos;

c) Providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;

d) Transferir progressivamente o serviço e os registros operacionais para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC CNDL RFB e ARs vinculadas;

e) Preservar qualquer registro não transferido a um sucessor;

f) Transferir, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e

g) Repassar à AC Raiz os documentos referentes aos certificados digitais e as respectivas chaves públicas, caso essas não sejam assumidas por outra AC.

5. CONTROLES PROCEDIMENTAIS

Nos itens seguintes da DPN estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC CNDL RFB e nas AR´S a ela vinculadas, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, foi estabelecido o número de pessoas requerido para sua execução.

5.1. PERFIS QUALIFICADOS

5.1.1. A AC CNDL RFB e AR´S vinculadas efetuam separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize o seu sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.1.2. A AC CNDL RFB e AR´S vinculadas estabelecem um mínimo de (03) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. O detalhamento dos perfis encontra-se em documento interno normativo.

5.1.3. Todos os operadores do sistema de certificação da AC CNDL RFB e AR´S vinculadas recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

5.1.4. Quando algum empregado se desligar da AR vinculada, suas permissões de acesso serão revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AR vinculada, suas permissões de acesso são revistas. Há uma lista de

revogação, com todos os recursos, antes disponibilizados, que o empregado deve devolver à AC e AR´S vinculadas no ato de seu desligamento.

5.2. NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

A AR´S vinculadas utilizam o requisito de controle multiusuário para a geração e a utilização da sua chave privada.

Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AR vinculada requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AR vinculada podem ser executadas por um único empregado.

5.2.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

5.2.1.1. Todo empregado das AR´S vinculadas tem sua identidade e perfil verificados antes de:

a) Ser incluído em uma lista de acesso às instalações da AC CNDL RFB;

b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC CNDL RFB;

c) Receber um certificado para executar suas atividades operacionais na AC CNDL RFB;

d) Receber uma conta no sistema de certificação da AC CNDL RFB.

5.2.1.2. Os certificados, contas e senhas utilizadas para identificação e autenticação dos empregados:

a) São diretamente atribuídos a um único empregado;

b) Não são compartilhados;

c) São restritos às ações associadas ao perfil para o qual foram criados.

5.2.1.3. As AR´s vinculadas implementam um padrão de utilização de "senhas fortes", definido na Política de Segurança implementada e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], juntamente com procedimentos de validação dessas senhas.

5.3. FUNÇÕES QUE REQUEREM SEPARAÇÃO DE DEVERES

As AR´S vinculadas impõe a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3.1. CONTROLES DE PESSOAL

Nos itens seguintes desta DPN são descritos os requisitos e procedimentos, implementados pela AC CNDL RFB, pelas AR´S e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os empregados da AC CNDL RFB e das AR´S vinculadas e PSS vinculados, 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.

5.3.2. ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE

Todo o pessoal da AC CNDL RFB e AR(s) Vinculada(s) envolvidos 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] e na Política de Segurança implementada pela AC.

5.3.3. PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

5.3.3.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AR Vinculada 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.

5.3.3.2. As AR´s vinculadas não definem requisitos adicionais para a verificação de antecedentes.

5.3.4. FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA

Todo o pessoal das AR´S Vinculadas envolvidas 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 CNDL RFB.

5.3.5. FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

A AC CNDL RFB e as AR(s) Vinculada(s) possuem pessoal e efetivo de contingência devidamente treinado, 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 das AR(s) Vinculada(s), a AC CNDL RFB suspenderá o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2. Os processos administrativos referidos acima contêm os seguintes itens:

a) Relato da ocorrência com “modus operandis”;

b) Identificação dos envolvidos;

c) Eventuais prejuízos causados;

d) Punições aplicadas se for o caso; e

e) Conclusões.

5.3.6.3. Concluído o processo administrativo, a AC CNDL RFB encaminha suas conclusões à AC Raiz.

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

a) Advertência;

b) Suspensão por prazo determinado; ou

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

5.3.7. REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

Todo o pessoal das AR(s) Vinculada(s) envolvidos 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] e na Política de Segurança implementada.

5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.3.8.1. A AC CNDL RFB torna disponível para todo o seu pessoal e para o pessoal da AR(s) vinculada(s):

a) Sua DPC AC CNDL RFB;

b) As PCs que implementa;

c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e a sua Política de Segurança;

d) Documentação operacional relativa a 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 CNDL RFB e é mantida atualizada.

5.4. TROCA DE CHAVE

5.4.1. Trinta dias antes da data de expiração do certificado digital, a AR Vinculada comunica ao seu titular, através do e-mail cadastrado no formulário de solicitação de certificado, a data de expiração do mesmo, junto com link https://www.spcbrasil.org.br/certificacaodigital/#certificados para a solicitação de novo certificado.

5.5. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

A AC CNDL RFB possui um Plano de Continuidade de Negócio, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos.

5.5.1. PROCEDIMENTOS GERENCIAMENTO DE INCIDENTE E COMPROMETIMENTO

5.5.1.1. A AC CNDL RFB possui um Plano de Continuidade do Negócio – PCN, de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. Possui ainda um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

5.5.1.2. Os procedimentos descritos no Plano de Continuidade do Negócio (PCN) da(s) AR(s) vinculada(s) contemplam a recuperação, total ou parcial das atividades das ARs, contendo, no mínimo as seguintes informações:

a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;

b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;

c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários;

d) Documentação dos processos e procedimentos acordados;

e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e

f) Teste e atualização dos planos.

6. CONTROLES DE SEGURANÇA

6.1. CONTROLES DE SEGURANÇA PARA AUTORIDADES DE REGISTRO

6.1.1. A AC CNDL RFB implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR Vinculadas para os processos de validação e aprovação de certificados.

6.1.2. São incluídos, no mínimo, os requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

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

6.1.2.2. As estações de trabalho da AR 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.

6.1.2.3. As estações de trabalho da AR contém apenas aplicações e serviços que são suficientes e necessários para as atividades corporativas.

6.1.2.4. As estações de trabalho da AR, 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 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, exceto para as atividades de suporte remoto;

j) Utilização de data e hora de Fonte Confiável do Tempo (FCT);

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;

m) Módulo de segurança, software assinado pela AC, que garanta a integridade e a segurança da estação de trabalho.

6.1.2.5. 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.

6.1.2.6. 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.

6.1.2.7. 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.

6.1.2.8. O aplicativo que faz interface entre a AR e o sistema de certificação da AC 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;

b) Acesso permitido somente a partir de equipamentos autenticados no sistema (ex. usando cadastramento prévio de endereço IP, certificado digital de equipamento ou outra solução que permita ao sistema identificar de forma unívoca o equipamento);

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.

6.1.2.9. 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, ou responsável designado, para colocar cada versão em ambiente de produção.

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

6.2. CONTROLES TÉCNICOS DO CICLO DE VIDA

Nos itens seguintes são descritos os controles implementados pela AC CNDL RFB e pelas AR´S a ela vinculadas no desenvolvimento de sistemas e no gerenciamento de segurança.

6.2.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.2.1.1. A AC CNDL RFB adota tecnologias de certificação digital e efetua as devidas customizações para adequar as necessidades do ambiente da AC, os quais são desenvolvidos por Analistas de Suporte, todos empregados de confiança de seu PSS. Estas customizações são realizadas inicialmente em um ambiente de desenvolvimento e depois de concluído, é colocado em um ambiente de homologação. Finalizado o processo de homologação é encaminhado um pedido para o Gerente da AC, que coordena o Processo de Certificação Digital que avaliam e decidem quanto a sua implementação.

6.2.1.2 Os processos de projeto e desenvolvimento conduzidos pela AC CNDL RFB provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC CNDL RFB.

6.3. CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.3.1. A AC CNDL RFB e AR´S vinculadas utilizam ferramentas e os procedimentos formais para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

6.3.2. A AC CNDL RFB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação.

7. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

A AC CNDL RFB, 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. TÓPICOS COBERTOS PELA AVALIAÇÃO

As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPC´S, PCs, PS´S, DPN´S e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo WebTrust.

A AC CNDL RFB 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.

As entidades da ICP-Brasil diretamente vinculadas a AC CNDL RFB, também receberam auditoria prévia, para fins de credenciamento. A AC CNDL RFB é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

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 ou de acesso à informação de status de certificado.

9.1.4. TARIFA PARA OUTROS SERVIÇOS

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

9.1.5. POLÍTICA DE REEMBOLSO

Item não aplicável.

9.2. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.2.1. ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

9.2.1.1. Como princípio geral, todo documento, informação ou registro fornecido à AC CNDL RFB ou às AR vinculadas é sigiloso.

9.2.1.2. Como princípio geral, nenhum documento, informação ou registro fornecido à AC CNDL RFB ou às AR´S vinculadas será divulgado.

9.2.2. INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

Os tipos de informações consideradas não sigilosas pela AC CNDL RFB e pelas ARs a ela vinculadas, compreendem, entre outros:

a) os certificados e as LCR´S/ OCSP emitidos pela AC CNDL RFB;

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

c) as PC´S implementadas pela AC CNDL RFB;

d) a DPC da AC CNDL RFB;

e) versões públicas de PS da AC CNDL RFB; e

f) a conclusão dos relatórios de auditoria da AC CNDL RFB.

9.3. RESPONSABILIDADE EM PROTEGER A INFORMAÇÃO CONFIDENCIAL

9.3.1. 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.

9.4. PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1. PLANO DE PRIVACIDADE

A AC CNDL RFB e AR´S vinculadas asseguram a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2. TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS

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

9.4.3. RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADA

A AC CNDL RFB e AR vinculadas são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.4. AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS

9.4.4.1. As informações privadas obtidas pela AC CNDL RFB e AR´S vinculadas poderão ser utilizadas ou divulgadas a terceiro mediante expressa autorização do respectivo titular, conforme legislação aplicável.

9.4.4.2. 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.

9.4.4.3. 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.

9.4.5. INFORMAÇÕES A TERCEIROS

Nenhum documento, informação ou registro sob a guarda das AR´S ou da AC CNDL RFB 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. DECLARAÇÕES E GARANTIAS

9.5.1. DECLARAÇÕES E GARANTIAS DA AR

Em acordo com item 4 desta DPN.

9.5.2. DECLARAÇÕES E GARANTIAS DO TITULAR

9.5.2.1 Toda informação necessária para a identificação do titular de certificado deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pelas AR´S vinculadas, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6. DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES

9.6.1. As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPN;

b) verificar, a qualquer tempo, a validade do certificado.

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

9.7. PRAZO E RESCISÃO

9.7.1. PRAZO

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

9.7.2. TÉRMINO

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

9.7.3. 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.

9.7.4. 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.

9.8. ALTERAÇÕES

9.8.1. MECANISMO DE NOTIFICAÇÃO E PERÍODOS

Mudança nesta DPN será publicado no site das AR´S vinculadas.

10. PRÁTICAS COMERCIAIS ARV´S

10.1. POLÍTICA DE GARANTIA

A Política de Garantia do SPC Brasil se estende a todos os seus clientes, sejam eles Pessoa Física ou Pessoa Jurídica, independentemente do tipo de produto adquirido. Sobre as senhas dos certificados, o SPC Brasil não mantém cópias ou métodos de recuperação de senhas PIN e PUK, dos dispositivos criptográficos, dessa forma, o cliente se torna totalmente responsável pelo uso do certificado.

Os cartões inteligentes ou Tokens são responsáveis pela geração do par de chaves e armazenamento do certificado digital. Ao digitar a senha PIN por (03) três vezes consecutivas de forma incorreta, a senha será bloqueada automaticamente e o desbloqueio ocorrerá somente através da senha PUK. Caso a senha PUK seja digitada por mais de (03) três vezes consecutivas incorretamente, a cartão ou token será bloqueada automaticamente.

As tentativas são cumulativas, ou seja, mesmo desconectando o dispositivo ou reiniciando o computador, a quantidade de tentativas não será zerada.

Mídias criptográficas

Nos casos onde forem identificados problemas ocasionados por mau uso da mídia criptográfica ou exclusão do conteúdo do certificado, não será oferecida a substituição e garantia. Nesse caso, haverá necessidade de aquisição de novo certificado conforme condições comerciais oferecidas pelos canais de venda disponíveis. Caso seja identificado pela área de suporte técnico defeitos de fabricação nas mídias criptográfica, durante o período de vigência da garantia, será realizada a troca do referido dispositivo, assim como a emissão de um novo certificado.

É importante salientar que a emissão do novo certificado digital, substituído em garantia, deverá seguir o processo de validação presencial, sendo gratuito nos pontos de atendimento da rede SPC Brasil.

Certificados tipo A1

O Certificado Digital do Tipo A1 é instalado diretamente no equipamento do titular, dessa forma, o cliente é responsável por armazená-lo em segurança, bem como as respectivas cópias (backup). O SPC Brasil não mantém cópias dos certificados ou senhas. Caso o equipamento do titular seja formatado, a recuperação do certificado será possível somente através da respectiva cópia, caso o cliente não a possua, será necessário realizar uma nova emissão. Os custos decorrentes dessa nova emissão correrão por conta do cliente.

Condições gerais A aplicação da política de garantia, sem custos ao cliente, está condicionada a autorização da área de operações de certificação digital, substituindo a mídia criptográfica ou o certificado conforme a necessidade.

Aceitando os termos de garantia do SPC Brasil, o consumidor abre mão de qualquer reclamação após o prazo de (180 dias). Para maiores informações sobre a política de garantia, estornos, atendimentos de suporte e esclarecimentos de dúvidas, entre em contato conosco através do telefone 3003-0633.

10.2. POLÍTICA DE ARREPENDIMENTO

De acordo com o artigo 49 do Código de Defesa do Consumidor, poderá ser exercido pelo cliente o direito de arrependimento da compra que for realizada na Plataforma E-Commerce / Loja

OnLine, no prazo de até 7 dias corridos, contados à partir da confirmação do pagamento pelo banco ou pela administradora do cartão de crédito.

O cliente deve solicitar o cancelamento através do email sac.cd@spcbrasil.org.br ou através do telefone (11) 3003-0633, Opção 1, com as seguintes informações:

• Nome completo:

• CPF: • E-mail:

• Banco: • Agência: • Conta:

• Protocolo de emissão do certificado:

• Motivo de Cancelamento:

• Número do Pedido: • Data de compra:

• Emissão do certificado já foi realizada?

A solicitação será considerada efetuada se o cliente tiver enviado todos os dados solicitados. Isto deve acontecer até o 7º dia corrido após o pagamento.

No caso de pagamentos realizados através de boleto bancário, será depositado o valor como crédito em conta corrente. Em pagamentos realizados através de cartão de crédito, será estornado o valor na próxima fatura. No caso de certificado já emitido, este será revogado no ato da solicitação apresentada pelo Cliente, responsabilizando-se o Cliente pela devolução das respectivas mídias junto ao ponto de atendimento onde foi realizada a emissão. Passado o 7º dia corrido após a confirmação do pagamento pelo banco ou pela administradora do cartão de crédito, não será possível exercer o direito de arrependimento. Caso o cliente queira cancelar o certificado após este período deverá observar as demais regras e políticas aplicáveis na Plataforma ECommerce / Loja OnLine.

11. DOCUMENTOS REFERENCIADOS

11.1. 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 http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[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