DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO

AC CNDL RFB

Versão 8.0 – Janeiro/ 2023

Sumário

VERSÃO	DATA	RESOLUÇÃO	ITEM ALTERADO
4.0	20/03/20	Resolução nº 151 de 30/05/2019; Resolução nº 154 de 01/10/2019; Resolução nº 155 de 03/12/2019	Diversos
4.0	20/03/20	Resolução nº 156 de 07/02/2020	Não se aplica
4.0	20/03/20	Instrução Normativa nº. 02	3.3.1.2 d; 3.3.2.3 e 3.3.2.4
4.1	13/10/20	Alteração dos links	1.3.1; 1.3.2.1; 1.3.5; 2.2.1;4.9.3.1; 5.6.1; 6.1.4 item c.
5.0	10/11/20	Resolução nº 177 de 20/10/2020	1.1.6 ; 1.3.2.1.c; 1.6; 3.2.a; 3.2.b; 3.2.1; 3.2.2.1.3 c; 3.2.2.1.5; 3.2.2.2; 3.2.3; 3.2.3.1.a; 3.2.3.1.e; 3.2.1.3.f; 3.2.3.1.3.b; 3.2.3.1.4; 3.2.3.1.7; 3.2.6; 3.2.8.3; 3.2.8.3.2; 3.2.8.4; 3.2.9.7; 3.2.9.8; 3.3.1.1; 3.3.1.2; 3.3.2.e; 3.3.2.f; 3.3.1.2.1; 3.3.1.3; 3.3.4;

			3.3.2; 3.3.2.1; 3.3.2.2; 3.3.2.3; 3.3.2.4; 4.1.2.4.c; 4.1.2.4.e ; 4.7; 4.9.1.3.b; 4.9.2.j; 4.9.3.3; 4.9.4.1; 5.4.6; 6.1.2; 6.2.4; 6.4.1.2; 6.5.3.2; 10.1; 10.5.
6.0	15/02/2021	Resolução CG ICP-Brasil nº 181 de 22/01/2021	3.2.3.1 e 3.2.3.1.8
7.0	10/12/2021	Resolução CG ICP-Brasil nº 197 de 16/11/2021	Título, súmario, 1.3.2.1, 1.5.3, 2.2.2, 3.2, 3.2.3, 3.2.3.1, 3.2.3.1.1, 3.2.3.1.8.1, 3.2.3.2.1 a 3.2.3.2.3.1, 3.2.8.2.1, 3.2.8.3.3, 3.2.8.4.2, 4.1, 4.1.2.2 y), 4.1.2.4 e), 4.9.3, 5.1.4, 5.1.6, 5.1.7, 5.4.1.6.1, 6.5.3.3, 7.1.9 e exclusão 10.2
8.0	17/01/2023	Resolução CG ICP-BRASIL N° 204	4.5.1.2 item b e f

Autor: Confederação Nacional de Dirigentes Lojistas - SPC Brasil

Edição: 17/01/2023

Versão: 8.0

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, AC integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução de seus serviços.

1.1.2. A elaboração desta DPC 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].

1.1.3. Item não aplicável

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

1.1.5. A AC CNDL RFB mantém todas as informações da sua DPC sempre atualizadas.

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

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1. Esta DPC "Declaração de Práticas de Certificação da Autoridade Certificadora CNDL RFB" referida a seguir simplesmente como "DPC-AC CNDL RFB" descreve as práticas e os procedimentos adotados pela AC CNDL RFB no âmbito da ICP-Brasil.

O OID da DPC-AC CNDL RFB atribuído pela AC Raiz após a conclusão do seu processo de credenciamento é **2.16.76.1.1.65.**

1.2.2. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC CNDL RFB, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes é: assinatura de documento e proteção de e-mail (S/MIME).

1.3 PARTICIPANTES DA ICP-BRASIL

1.3.1 Autoridade Certificadora (AC)

Esta DPC está relacionada à AC CNDL RFB e encontra-se publicada em sua página web https://www.spcbrasil.org.br/certificacaodigital/suporte/duvidas-frequentes. A AC CNDL RFB para a Secretaria da Receita Federal do Brasil está no nível imediatamente subsequente ao da Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB).

Com relação aos tipos específicos de certificado emitidos pela AC CNDL RFB para a Secretaria da Receita Federal do Brasil, referida a seguir como "AC CNDL RFB", devem ser consultadas as Políticas de Certificado

da AC CNDL RFB (http://repositorio.acspcbrasil.org.br/ac-cndlrfb/ac-cndl-rfb-dpc.pdf), que explicam como um tipo específico de certificado é gerado e administrado pela AC CNDL RFB e utilizado pela comunidade.

1.3.2 Autoridade de Registro (AR)

1.3.2.1. 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´S credenciadas, **e;**

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

1.3.3 Titulares do Certificado

Podem ser titulares de certificados emitidos pela AC CNDL RFB, 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.

1.3.4 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, vinculados à AC CNDL RFB estão relacionados na página https://www.spcbrasil.org.br/certificacaodigital/suporte/duvidas-frequentes

1.4 USABILIDADE DO CERTIFICADO

1.4.1 Uso apropriado do certificado

A AC CNDL RFB pratica as seguintes Políticas de Certificado Digital:

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

Nas PC´S 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 existem restrições ou proibições para o uso desses certificados, estão listados nas PC´S implementadas pela AC CNDL RFB.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 Organização Administrativa do Documento

Nome da AC: AC CNDL RFB

1.5.2 Contatos

- Rua: Leôncio de Carvalho nº 234 – 13º Andar
- CEP: 04003-010
- Paraiso - São Paulo, SP
- Telefones: (5511) 3549-6800 / 3003-0633
- Área para contato: Serviço de Atendimento ao Cliente.
- E-mail: sac.cd@spcbrasil.org.br
- Pág. Web: www.spcbrasil.org.br

1.5.3 Pessoa que determinada a adequabilidade da DPC com a PC

Nome: Marli Paiva Rubio ou Vanessa Danielle Rocha Berloni

Telefone: (11) 3549-6800

E-mail: compliance@spcbrasil.org.br

Outros: Setor de Compliance & Controles Internos da AC CNDL RFB

1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI. Os procedimentos de aprovação da DPC da AC CNDL RFB 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
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
CSR	Certificate Signing Request
DETRAN	Departamento Nacional de Trânsito
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	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
PIN	Personal Identification Number
PIS	Programa de Integração Social
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
PUK	PIN Unbloking Key
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSE	Tribunal Superior Eleitorial
UF	Unidade de Federação
URL	Uniform Resource Locator

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 DA AC CNDL RFB

As obrigações da AC CNDL RFB em relação ao seu repositório estão abaixo relacionadas:

a) Disponibilizar logo após a emissão os certificados emitidos pela AC CNDL RFB e sua LCR;

b) Publicar em sua página web, sua DPC-AC CNDL RFB e as PC´S aprovadas que implementadas;

c) Publicar, em página web, informações sobre o descredenciamento de AR;

d) Estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana; e

e) Implementar os recursos necessários para a garantia da segurança dos dados nele armazenados.

2.1.2. Neste item foram descritos os requisitos aplicáveis aos repositórios utilizados pela AC CNDL RFB, tais como:

a) Localização Física e Lógica: ambiente de nível 4 e de rede independente

b) Disponibilidade: 24 (vinte e quatro) horas por dia 7 (sete) dias por semana

c) Protocolos de acesso: http

d) Requisitos de Segurança: Somente a AC CNDL RFB por seus funcionários qualificados e designados especialmente para este fim, poderão efetuar atualizações nas informações por ela publicadas em seu repositório. Cada computador servidor da AC CNDL RFB, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, inclusive o servidor de repositório, implementa os controles descritos no item 6.5 desta DPC.

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

2.1.4. A AC CNDL RFB disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR.
http://repositorio.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv5.crl

http://repositorio2.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv5.crl

2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.2.1. A AC CNDL RFB publica e mantém disponível em seu site https://www.spcbrasil.org.br/certificacaodigital/suporte/duvidas-frequentes informações com disponibilidade mínima de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia (7) sete dias por semana.

2.2.2. As seguintes informações, no mínimo, são publicadas pela AC CNDL RFB em página Web:
a) Seu próprio certificado;

b) Suas LCR´S;

c) Sua DPC- AC CNDL RFB;

d) As PCs que implementa;

e) A DPC da AC RFB está disponível no site da AC-RFB (http://hom.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf);

e) Uma relação, regularmente atualizada, contendo as AR´S vinculadas e seus respectivos endereços;

f) Uma relação, regularmente atualizada, contendo os PSS´S vinculados.

2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

Certificados da AC CNDL RFB são publicados imediatamente após sua emissão. A publicação da LCR se dá conforme determinado na PC correspondente. As versões ou alterações desta DPC e das PCs, assim como os endereços das AR´S vinculadas, são atualizados no site da AC CNDL RFB após aprovação da AC Raiz da ICP - Brasil.

A AC CNDL RFB atualiza as informações acima tão logo sejam geradas, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

2.4 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 DPC-AC CNDL RFB e nas Políticas de Certificados que implementa, após haver obtido a competente autorização do CG da ICP-Brasil.

Somente a AC CNDL RFB, por seus funcionários competentes e designados especialmente para esse fim, poderão efetuar as necessárias atualizações de suas LCR.

O certificado da AC CNDL RFB e os certificados emitidos pela AC CNDL RFB não podem ser modificados. Caso se faça necessário modificar os dados contidos nos mesmos, será necessária a revogação dos certificados.

Não há restrições para o acesso da leitura desta DPC-AC CNDL RFB, das PCs e das LCR´S. Todas as informações disponibilizadas pela AC CNDL RFB, estão disponíveis para leitura sem restrições.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC CNDL RFB verifica 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 AC CNDL RFB 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 AC CNDL RFB emite certificados com nomes que permitam a identificação unívoca. Para isso utiliza o "distinguished name" do padrão ITU X.500, seguindo os padrões estabelecidos pelo documento LEIAUTE DOS CERTIFICADOS DIGITAISDA SECRETARIA DA RECEITA FEDERAL DO BRASIL [12]. 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. Informações específicas, estão descritas nas PC´S implementadas da AC CNDL RFB.

3.1.1.2. Item não aplicável

3.1.2 Necessidade de nomes serem significativos

3.1.2.1. A AC CNDL RFB faz 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 CNDL RFB.

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 nomes

3.1.4.1. Item não aplicável.

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

3.1.5 Unicidade de Nomes

Os identificadores 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 procedimentogarante a unicidade de todos os nomes no âmbito da AC CNDL RFB.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

Tais procedimentos serão analisados com base na legislação em vigor.

3.2 VALIDAÇÃO INICIAL DE IDENTIDADE

A AC CNDL RFB e as AR´S vinculadas utilizam os seguintes requisitos e procedimentos para realização dos 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., 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.

b) Emissão do Certificado: após a 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 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 o controle 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

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

3.2.2.1.2. 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.

3.2.2.1.3. A AC CNDL RFB 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 no termo de titularidade de que trata o item 4.1. pelo titular ou responsável pelo uso do certificado.

Nota 1: A AR poderá solicitar uma assinatura manuscrita ao responsável pelo 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 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 daidentidade 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 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. 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.

3.2.2.3.2. Cada 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, 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 de uso indicado no certificado.

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) Item não aplicável.

b) Por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz; ou

c) Item não aplicável.

3.2.3.1. Procedimentos para 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 o digital:

i. Registro de Identidade, se brasileiro;

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

iii. Passaporte, se estrangeiro não domiciliado no Brasil;

iv. Título de eleitor com foto;

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

NOTA 1: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais 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: Os documentos que possuem data de validade precisam estar dentro prazo. Excepcionalmente a CNH, poderá ser aceita para identificação de titular de certificado digital.

NOTA 3: a AC CNDL RFB 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 CNDL RFB.

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.

NOTA 6: 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, fica dispensada a apresentação de qualquer dos documentos elencados no item 3.2.3.1. 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 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) pela AR ou AR própria da AC ou ainda AR própria do PSS da AC; 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. Item não aplicável.

3.2.3.1.6. Item não aplicável.

3.2.3.1.7. Item não aplicável.

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.

3.2.3.1.8.1. Item não aplicável.

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) Cadastro de Pessoa Física (CPF);

b) Nome completo, sem abreviações;

c) Data de nascimento.

d) E-mail.

3.2.3.2.1.1. Item não aplicável.

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

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

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

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.

3.2.3.2.3.1. Item não aplicável.

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

Item não aplicável.

3.2.5 Validação das Autoridades

Item não aplicável.

3.2.6 Critérios para Interoperação

Item não aplicável.

3.2.7 Autenticação da Identidade de Equipamento ou Aplicação

Item não aplicável.

3.2.8 Procedimentos Complementares

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

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 CNDL RFB, 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 deverá 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.

3.2.8.2.1. Item não aplicável.

3.2.8.3. A AC CNDL RFB mantém 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.

3.2.8.3.1. Item não aplicável.

3.2.8.3.2. Item não aplicável.

3.2.8.3.3. Item não aplicável.

3.2.8.4. A AC CNDL RFB disponibiliza, 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 no documento 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.

3.2.8.4.1. 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.

3.2.8.4.2. Item não aplicável.

3.2.9 Procedimentos Específicos

3.2.9.1. Item não aplicável.

3.2.9.2. Item não aplicável.

3.2.9.3. Item não aplicável.

3.2.9.4. Item não aplicável.

3.2.9.5. Item não aplicável.

3.2.9.6. Item não aplicável.

3.2.9.7. Item não aplicável.

3.2.9.8. Item não aplicável.

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1 Identificação e Autenticação para rotina de novas chaves antes da expiração

3.3.2. Esta DPC estabelece os métodos de identificação do solicitante utilizados pela AC CNDL RFB para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

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

a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;

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 res pectivo 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; ou

f) Item não aplicável.

3.3.2.1. Item não aplicável.

3.3.3. Não existem procedimentos específicos descritos na PC da AC.

3.3.4. Item não aplicável.

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, ou seja, cadastrados na AR.

3.4.2. Os procedimentos para solicitação de revogação de certificado estão descritos no item 4.9.3 desta DPC. 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 CNDL RFB 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, conforme item 3.2;

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;

c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo certificado no caso de pessoa Jurídica, elaborados conforme o documento TERMO DE TITULARIDADE [4] específico.

d) A confirmação de cadastro por videoconferência realizada por agente de registro devidamente habilitado e autorizado, nas situações descritas nos itens 3.3.2.3 e 3.3.2.4. 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 requere nte a ser identificada;
d.4) Os AGR´S das AR´S vinculadas a AC CNDL, certificam-se sobre a veracidade da informação contida no documento de identificação do requerente, quando um documento de identificação for utilizado.

e) Item não aplicável.

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.

4.1.1 Quem pode submeter uma solicitação de Certificado

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. A submissão da solicitação deve ser sempre por intermédio da AR vinculada, através de agente de registro devidamente autorizado.

4.1.1.1 Item não aplicável.

4.1.1.2 Item não aplicável.

4.1.1.3. Item não aplicável.

4.1.1.4. Item não aplicável.

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 PC´S implementadas.

4.1.2.1. Responsabilidades da AC

4.1.2.1.1 A AC CNDL RFB é responsável e responde pelos danos a que der causa.

4.1.2.1.2. A AC CNDL RFB responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR´S subordinadas e PSS.

4.1.2.1.3. Item não aplicável.

4.1.2.2. Obrigações da AC

a) operar de acordo com a sua DPC e com as PC`S que implementa;

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

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC de nível superior, 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 usuários finais;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas LCR´S;

k) publicar em sua página web sua DPC e as PC´S aprovadas que implementa;

l) publicar, em sua página web, as informações definidas no item 2.2.2 deste documento;

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 AR´S, 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 AC´S que utilizam de seus serviços; e

y) Item não aplicável.

4.1.2.3. Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

4.1.2.4. Obrigações das AR´S

Neste item estão contempladas as obrigações das AR´S 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 CNDL RFB 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 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 as AR´S a ela vinculadas executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2 Aprovação ou Rejeição de pedidos de certificado

4.2.2.1. Item não aplicável

4.2.2.2. A AC CNDL RFB e AR´S a ela vinculada podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

4.2.3 Tempo para processar a solicitação de certificado

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

4.3 EMISSÃO DE CERTIFICADO

4.3.1 Ações da AC 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; e 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

A notificação de emissão de certificados emitidos pela AC CNDL RFB 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 deveresimpostos pelo Termo de Titularidade, pela PC implementada e por esta DPC;

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 DPC;

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.

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

4.4.2 Publicação do Certificado pela AC CNDL RFB

O certificado da AC CNDL RFB é publicado de acordo com item 2.2 desta DPC.

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

A notificação se dará de acordo com item 2.2 desta DPC.

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

A AC CNDL RFB opera 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 nesta 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, constantes dos termos de titularidade de que trata o item 4.1, 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 privadascódigo de ativação (PIN) e dispositivos criptográficos;

c) Utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto pelas PC´S e DPC correspondentes;

d) Conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC´S correspondentese por outros documentos aplicáveis da ICP-Brasil; e

e) Informar à AC CNDL RFB qualquer comprometimentode sua chave privada e solicitar a imediata revogação do certificado correspondente.

f) garantir a proteção do PUK, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente, quando aplicável.

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

4.5.2 Usabilidade da Chave Pública de do Certificados das Partes Confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6 RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPC.

4.6.1 Circunstâncias para renovação dos Certificados

Em acordo com item 3.3 desta DPC.

4.6.2 Quem pode solicitar a Renovação

Em acordo com item 3.3 desta DPC.

4.6.3 Processamento de requisição para Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.4 Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com item 3.3 desta DPC.

4.6.6 Publicação de uma renovação de um certificado pela AC CNDL RFB

Item não aplicável.

4.6.7 Notificação de emissão de Certificado pela AC CNDL RFB para outras entidades

Em acordo com item 4.3 desta DPC.

4.7 NOVA CHAVE DE CERTIFICADO (Re-key)

Item não aplicável.

4.8 MODIFICAÇÃO DE CERTIFICADO

Item não aplicável.

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1 Circunstâncias para revogação

4.9.1.1. A AC CNDL RFB, nesta DPC evidencia as circunstâncias nas quais um certificado poderá ser revogado.

4.9.1.2. Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

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

b) Quando for necessário alterar qualquer informação constante no certificado; ou

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

d) No caso dissolução da AC CNDL RFB;

e) No caso de falecimento do titular - pessoas físicas ou demissão do responsável por pessoas jurídicas;

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) Por decisão judicial.

4.9.1.3. Deve-se observar ainda que:

a) A AC CNDL RFB revogará, no prazo definido no item 4.9.3.3 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 CNDL RFB caso esta deixe 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.

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

4.9.1.4.1. Item não aplicável.

4.9.1.4.2. Item não aplicável.

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

4.9.2 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) Por determinação da AC CNDL RFB;

e) Pela AR Vinculada que recebeu a solicitação; ou

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

g) Item não aplicável;

h) Item não aplicável;

i) Item não aplicável.

j) Item não aplicável.

4.9.3 Procedimento para solicitação de revogação

4.9.3.1. 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.

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

4.9.3.2. Como diretrizes gerais:

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

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

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

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

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

4.9.3.4. Item não aplicável.

4.9.3.5. A AC CNDL RFB responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.9.3.6. Item não aplicável.

4.9.4 Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1. e deve estabelecer o prazo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado poderá ser solicitada sem cobrança de tarifa pela AC.

4.9.4.2. 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.

4.9.5 Tempo em que a AC CNDL RFB dever processar o pedido de revogação

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

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7 Frequência de emissão de LCR

4.9.7.1. A frequência de emissão da LCR da AC CNDL RFB referente a certificados de usuários finais é de 1 hora.

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

4.9.7.3. Item não aplicável.

4.9.7.4. Item não aplicável.

4.9.7.5. Item não aplicável.

4.9.8 Latência máxima para a LCR

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

4.9.9 Disponibilidade para revogação/ verificação de status on-line

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

4.9.10 Requisitos para verificação de revogação on-line

Item não aplicável.

4.9.11 Outras formas disponíveis para divulgação de revogação

Item não aplicável.

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. Havendo roubo, perda, modificação, acesso indevido ou qualquer forma de comprometimento da chave privada ou de sua mídia, o titular do certificado deve comunicar imediatamente a AC CNDL RFB, de maneira escrita, solicitando a revogação de seu certificado.

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

4.9.13 Circunstâncias para suspensão

Item não aplicável.

4.9.14 Quem pode solicitar suspensão

Item não aplicável.

4.9.15 Procedimento para solicitação de suspensão

Item não aplicável.

4.9.16 Limites no período de suspensão

Item não aplicável.

4.10 SERVIÇOS DE STATUS DE CERTIFICADO

4.10.1. Características operacionais

A AC CNDL RFB fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados, conforme item 4.9.

4.10.2. Disponibilidade dos serviços

Ver item 4.9

4.10.3. Funcionalidades Operacionais

Ver item 4.9

4.11 ENCERRAMENTO DE ATIVIDADES

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

4.11.2. 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 AR´S 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.

h) Comunicar os usuários sobre a extinção dos serviços através de publicação em jornal de grande circulação.

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

Não é permitida a custódia (Escrow) das chaves privadas da AC CNDL RFB.

4.12.1 Política e práticas de custódia e recuperação de chave

Item não aplicável.

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

Item não aplicável.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES

São implementados pela AC CNDL RFB os controles descritos a seguir para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 CONTROLES FÍSICOS

Os controles físicos referentes às instalações que abrigam os sistemas da AC CNDL RFB, estão descritos nos itens a seguir.

5.1.1 Construção e localização das instalações

5.1.1.1. A localização e o sistema de certificação da AC CNDL RFB não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não são admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Na construção das instalações da AC CNDL RFB foram considerados, entre outros, os seguintes aspectos relevantes para os controles de segurança física:

- Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, nobreaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;

- Instalações para sistemas de telecomunicações;

- Existem sistemas de aterramento e de proteção contra descargas atmosféricas;

- Existe Iluminação de emergência em todos os níveis e áreas cobertas por câmeras de monitoramento.

5.1.2 Acesso físico

A AC CNDL RFB implantou um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a Política de Segurança implementada e os requisitos que seguem.

5.1.2.1 Níveis de acesso

5.1.2.1.1. A AC CNDL RFB definiu 4 (quatro) níveis de acesso físico aos diversos ambientes, e 2 (dois) níveis relativos à proteção da chave privada da AC CNDL RFB.

5.1.2.1.2. O primeiro nível - ou nível 1 - situa-se após a primeira barreira de acesso às instalações da AC CNDL RFB. Para entrar em uma área de nível 1, cada indivíduo deve ser identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação da AC CNDL RFB devem transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC CNDL RFB é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC CNDL RFB, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível - ou nível 2 - é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico, e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC CNDL RFB.

5.1.2.1.5. O terceiro nível - ou nível 3 - situa-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC CNDL RFB. As atividades relativas ao ciclo de vida dos certificados digitais estão localizadas a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não podem permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6. No terceiro nível (nível 3) são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: cartão eletrônico individual e identificação biométrica.

5.1.2.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC CNDL RFB, não são admitidos a partir do nível 3 (três).

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC CNDL RFB tais como emissão e revogação de certificados, e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividadesestão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9. No quarto nível todas as paredes, piso e teto são revestidosde aço e concreto ou de outromaterial de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Noquarto nível, os dutos de refrigeração e de energia,

bem como os dutos de comunicação, não permitem a invasão física da área de quarto nível. Adicionalmente, esse ambiente de nível 4 (quatro) possui proteção contra interferência eletromagnética externa.

5.1.2.1.10. As salas-cofre foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

5.1.2.1.11. Na AC CNDL RFB há 1 (um) ambiente de quarto nível para abrigar e segregar, respectivamente:

- Equipamentos de produção on-line e cofre de armazenamento;
- Equipamentos de produção off-line e cofre de armazenamento.
- Equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

5.1.2.1.12. O quinto nível(nível 5), O quinto nível - ou nível 5 (cinco), interior ao ambiente de nível 4 (quatro), compreende um cofre que armazena:
a) Backups das chaves criptográficas da AC CNDL RFB;
b) Dados de ativação destas chaves; e
c) Documentos necessários para a ativação da contingência do ambiente, caso necessário.

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre obedece às seguintes especificações mínimas:

- É feito em aço ou material de resistência equivalente;
- Possui tranca com chave e segredo.

5.1.2.1.14. O sexto nível (ou nível 6), consiste em pequenas caixas de aço localizadas no interior do cofre de quinto nível. Cada uma dessas caixas dispõe de uma fechadura individual. Os dados de ativação da chave privada da AC CNDL RFB são armazenados nessas caixas.

5.1.2.2 Sistemas físicos de detecção

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

5.1.2.2.2. Os arquivos de imagens resultantes da gravação 24 x 7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, um arquivo referente a cada semana. Essas gravações são armazenadas em ambiente quarto nível.

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

5.1.2.2.4. No ambiente de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não é satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais empregados, o

critério mínimo de ocupação deixa de ser satisfeito, ocorre a reativação automática dos sensores de presença.

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

5.1.2.2.6. Os sistemas de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujoposicionamento permite o acompanhamento das ações.

5.1.2.3 Sistema de Controle de acesso

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

5.1.2.4 Mecanismos de emergência

5.1.2.4.1. Mecanismos específicos foram implantados pela AC CNDL RFB para garantir a segurança de seu pessoal e de seus equipamentos emsituações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência são documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.3 Energia e ar condicionado

5.1.3.1. A infraestrutura do ambiente de certificação da AC CNDL RFB foi dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC CNDL RFB e seus respectivos serviços. Um sistema de aterramento foi implantado.

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

5.1.3.3. Foram utilizados tubulações, dutos, calhas, quadros e caixas - de passagem, distribuição e terminação - projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. Foram utilizados dutos separados para os cabos de energia, de telefonia e de dados.

5.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

5.1.3.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Qualquer modificação nessa rede é previamente documentada.

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

5.1.3.7. O sistema de climatização atende os requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é tolerante a falhas.

5.1.3.8. A temperatura do ambiente de nível 4, é atendida pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9. O sistema de ar condicionado é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC CNDL RFB é garantida, por meio de:

- Geradores de porte compatível;
- Geradores de reserva;
- Sistemas de nobreaks redundantes;
- Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

5.1.5 Prevenção e proteção contra incêndio

5.1.5.1. Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2. Nas instalações da AC CNDL RFB não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. O ambiente de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso ao ambiente de nível 4 constituem eclusas, onde uma porta só se abre quando a anterior estiver fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC CNDL RFB, o aumento da temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, 1 (uma) hora.

5.1.6 Armazenamento de mídia

São observados os critérios estabelecidos na norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7 Destruição de lixo

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

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

5.1.8 Instalações de Segurança (BACKUP) externas (OFF-SITE) para AC

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

5.2 CONTROLES PROCEDIMENTAIS

Nos itens seguintes da DPC 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.

5.2.1 Perfis qualificados

5.2.1.1. A AC CNDL RFB efetua 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.

5.2.1.2. A AC CNDL RFB estabelece 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.

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

5.2.1.4. Quando um empregado se desligar da AC CNDL RFB, suas permissões de acesso são revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC CNDL RFB, suas permissões de acesso são revistas. Há uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deve devolver à AC no ato de seu desligamento.

5.2.2 Número de pessoas necessárias por tarefa

5.2.2.1. A AC CNDL RFB utiliza o requisito de controle multiusuário para a geração e a utilização da sua chave privada, na forma definida no item 6.2.2.

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

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC CNDL RFB 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.

5.2.3.2. 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.

5.2.3.3. A AC CNDL RFB implementa 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.

5.2.4 Funções que requerem separação de deveres

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

5.3 CONTROLES DE PESSOAL

Nos itens seguintes desta DPC são descritos os requisitos e procedimentos, implementados pela AC CNDL RFB, pelas AR´S e PSS vinculado 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 vinculado, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

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

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

c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de Idoneidade

Todo o pessoal da AC CNDL RFB e das AR´S Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP -BRASIL [8] e na Política de Segurança implementada pela AC.

5.3.2 Procedimento de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC CNDL RFB e das AR`S Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido a:

a) Verificação de antecedentes criminais;

b) Verificação de situação de crédito;

c) Verificação de histórico de empregos anteriores;

d) Comprovação de escolaridade e de residência.

5.3.2.2. A AC CNDL RFB não define requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal da AC CNDL RFB e das AR`S Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e mecanismos de segurança da AC CNDL RFB e das AR`S vinculadas;

b) Sistema de certificação em uso na AC CNDL RFB;

c) Procedimentos de recuperação de desastres e de continuidade do negócio;

d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.2 e 3.2.3; e

e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC CNDL RFB e das AR´S Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamentode certificados é mant ido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC CNDL RFB e das AR´S Vinculadas.

5.3.5 Frequência e sequência de rodízio de cargos

A AC CNDL RFB e a AR`S Vinculadas 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 da AC CNDL RFB e da AR´S Vinculadas, a AC CNDL RFB ou a AR Vinculada 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 RFB e 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 da AC CNDL RFB e da AR`S Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme é 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 a ela vinculadas:

a) Sua DPC AC CNDL RFB;

b) As PC´S que implementa;

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

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 PROCEDIMENTOS DE LOG DE AUDITORIA

Nos itens seguintes da DPC são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC CNDL RFB com o objetivo de manter um ambiente seguro.

5.4.1 Tipos de eventos registrados

5.4.1.1. A AC CNDL RFB registra em arquivos de auditoria os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são incluídos em arquivos de auditoria:

a) Iniciação e desligamento do sistema de certificação;

b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC CNDL RFB;

c) Mudanças na configuração da AC CDL RFB ou nas suas chaves;

d) Mudanças nas políticas de criação de certificados;

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

f) Tentativas não-autorizadas de acesso aos arquivos de sistema;

g) Geração de chaves próprias da AC CNDL RFB ou de usuários finais;

h) Emissão e revogação de certificados;

i) Geração de LCR;

j) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;

k) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e

l) Operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1. Item não aplicável

5.4.1.2. A AC CNDL RFB registra, eletrônica ou manualmente, as seguintes informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

a) Registros de acessos físicos;

b) Manutenção e mudanças na configuração de seus sistemas;

c) Mudanças de pessoal e de perfis qualificados;

d) Relatórios de discrepância e comprometimento; e

e) Registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.3. A AC CNDL RFB não registra outras informações.

5.4.1.4. Os registros de auditoria, eletrônicos ou manuais, contém a data e a hora do evento registrado e a identidade do agente que o causou.

5.4.1.5. No intuito de facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC CNDL RFB é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.1.6. A AC CNDL RFB registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos estão obrigatoriamente incluídos em arquivos de auditoria:

a) Os agentes de registro que realizaram as operações;

b) Data e hora das operações;

c) A associação entre os agentes que realizaram a validação e aprovação e o certificado gerado;

d) A assinatura digital do executante.

5.4.1.6.1. Item não aplicável.

5.4.1.7. A AC CNDL RFB define, em documento disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2 Frequência de auditoria de registros

A análise dos registros correspondentes à auditoria da AC CNDL RFB é feita periodicamente, não sendo superior a uma semana. Essa análise envolve também uma inspeção breve de todos os registros, com a verificação de que não foram alterados, e é seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3 Período de retenção para registros de auditoria

A AC CNDL RFB mantém em suas próprias instalações localmente seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena os seus registros de auditoria da maneira descrita no item 5.5.

5.4.4 Proteção de registro de auditoria

5.4.4.1. O sistema de registro de eventos de auditoria da AC CNDL RFB inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção, através das funcionalidades nativas dos sistemas operacionais.

5.4.4.2. Mecanismos obrigatórios de proteção de informações utilizados:

a) Os acessos lógicos são liberados através da ferramenta nativa do sistema operacional de modo a assegurar o uso apenas a usuários ou processos autorizados;

b) Os acessos lógicos aos registros de eventos de auditoria são registrados em logs do próprio sistema operacional;

c) Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

5.4.4.3. Os mecanismos de proteção descritos neste item obedecem à Política de Segurança implementada, de conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.5 Procedimentos para cópia de segurança (BACKUP) de registro de auditoria

É gerado pela AC CNDL RFB semanalmente cópia de backup de seus registros de auditoria, através de procedimentos utilizando conexão segura.

5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)

O sistema de coleta de dados de auditoria é interno à AC CNDL RFB e utiliza processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.7 Notificação de agentes causadores de eventos

No momento em que um evento é registrado pelo conjunto de sistemas de auditoria da AC CNDL RFB, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8 Avaliações de vulnerabilidade

Os possíveis eventos de vulnerabilidade detectados na análise periódica dos registros de auditoria da AC CNDL RFB, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são tomadas pela AC CNDL RFB e registradas para fins de auditoria.

5.5 ARQUIVAMENTO DE REGISTROS

5.5.1 Tipos de registros arquivados

Os tipos de eventos arquivados pela AC CNDL RFB, são:

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC CNDL RFB;

g) Informações de auditoria previstas no item 5.4.1.

5.5.2 Período para retenção de arquivo

Os períodos de retenção para cada evento arquivado, são:

a) As LCR´S e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;

b) Os dossiês dos titulares devem ser retidos, no mínimo, por 07 (sete) anos, a contar da data de expiração ou revogação do certificado.

c) As demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

5.5.3 Proteção de arquivo

Os registros arquivados da AC CNDL RFB são classificados e armazenados com requisitos de segurança compatíveis com essa classificação e com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.5.4 Procedimentos de cópia de arquivo

5.5.4.1. Uma segunda cópia de todo o material arquivado será armazenada no site backup, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

5.5.4.3. A AC CNDL RFB verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5 Requisitos para datação de registros

Os servidores estão sincronizados com a hora Greenwich Mean Time (GMT). Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT no formato DD/MM/AAAA HH:MM:SS, inclusive os certificados emitidos por esses equipamentos.
No caso dos registros feitos manualmente e formulários de requisição de certificados, estes contêm a Hora Oficial do Brasil.

5.5.6 Sistema de coleta de dados de arquivo (interno e externo)

Todos os sistemas de coleta de dados de arquivo utilizados pela AC CNDL RFB em seus procedimentos operacionais são automatizados e manuais e internos, e executados por seu pessoal operacional ou por seus sistemas.

5.5.7 Procedimentos para obter e verificar informações de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC CNDL RFB ou à AR Vinculada, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

5.6 TROCA DE CHAVE

5.6.1. Trinta dias antes da data de expiração do certificado digital, a AR 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.

5.6.2. Item não aplicável.

5.7 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.

5.7.1 Procedimentos gerenciamento de incidente e comprometimento

5.7.1.1. 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.

5.7.1.2. Os procedimentos descritos no Plano de Continuidade do Negócio (PCN) das AR´S vinculadas contemplam a recuperação, total ou parcial das atividades das AR´S, 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.

5.7.2 Recursos computacionais, Softwares e/ ou dados corrompidos

5.7.2.1. Os procedimentos de recuperação utilizados pela AC CNDL RFB, quando recursos computacionais, softwares ou dados estiverem corrompidos ou houver suspeita de corrupção, incluem, mas não se limitam a somente estes:

I - A identificação da crise;

II - Acionamento dos principais gestores;

III - Ativação das equipes;

IV - Contenção da crise;

V - Estimativa do alargamento da crise;

VI - Declaração do início das atividades de ativação da situação de recuperação;

VII - Notificação da crise;

VIII - Registro da crise; e

IX - Crítica para melhoria.

5.7.2.2. Nas situações de crise relacionadas aos recursos computacionais, software e dados corrompidos ou quando houver suspeita de corrupção desses componentes, após a identificação da crise ou confirmação da suspeita de corrupção, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de corrupção.

5.7.2.3. Os procedimentos de recuperação dos recursos computacionais, softwares e dados corrompidos envolvem: identificação da necessidade de recurso computacional alternativo e, em caso de necessidade, disponibilização de outro recurso computacional equivalente, instalação dos softwares necessários e recuperação dos dados através do arquivo de back-up, conforme detalhado no Plano de Continuidade de Negócios da ECDS e no Plano de Migração e Fluxo de Ativação do Ambiente Backup.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado de entidade é revogado

Em caso de revogação do certificado da AC CNDL RFB, após a identificação do imprevisto, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados dos usuários finais, é gerado um novo par de chaves da AC CNDL RFB, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para os usuários finais.

5.7.3.2 Chave de entidade é comprometida

Em caso de comprometimento da chave da AC CNDL RFB, após a identificação da crise são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os

certificados da AC CNDL RFB e dos usuários finais, é gerado um novo par de chaves, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para os usuários finais.

5.7.4 Capacidade de continuidade de negócio após desastre

Em caso de desastre natural ou de outra natureza, após a identificação da crise são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de exposição e comprometimento do ambiente. Na confirmação do incidente e constatado impossibilidade de operação no site, as atividades são transferidas para o site de contingência/ recuperação de desastre.

5.8 EXTINÇÃO DA AC

Em caso de extinção da AC CNDL RFB serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 Geração do par de chaves

6.1.1.1. O par de chaves criptográficos da AC CNDL RFB é gerado pela própria AC CNDL RFB em módulo criptográfico de hardware, com certificação INMETRO no padrão obrigatório, conforme definido no DOC-ICP-01.01, após o deferimento do seupedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil. Este processo é realizado no ambiente de nível 4 (quatro) na presença de múltiplas pessoas de confiança e treinados para esta função, seguindo procedimento formalizado e auditável.

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

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

6.1.1.4. O processo de geração do par de chaves da AC CNDL RFB é feito por hardware.

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

6.1.1.6 O módulo criptográfico utilizado para armazenamento da chave privada da AC CNDL RFB possuí Certificação INMETRO, conforme indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.2 Entrega da chave privada à entidade

A geração e a guarda de uma chave privada são de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3 Entrega da chave pública para o emissor do certificado

6.1.3.1. Para a entrega de sua chave pública AC CNDL RFB Certificadora Principal, encarregada da emissão de seu certificado, a AC CNDL RFB fará uso do padrão PKCS#10.

6.1.3.2. Os procedimentos para a entrega da chave pública de um solicitante de certificado à AC CNDL RFB, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer. Os procedimentos estão detalhados em cada PC implementada.

6.1.4 Entrega da chave pública da AC às terceiras partes

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

a) No momento da disponibilização de um certificado para seu titular, usando formato definido no documento PADRÕES E ALGORITIMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].;

b) Diretório;

c) página Web da AC CNDL RFB (https://www.spcbrasil.org.br/certificacaodigital/suporte/duvidas-frequentes);

d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil

e) Repositório da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1. Cada PC implementada pela AC CNDL RFB define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2. Item não aplicável.

6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros

6.1.6.1. A AC CNDL RFB adota o padrão FIPS (Federal Information Processing Standard) 140-2, nível 3 (para as cadeias de certificação V2 e V5) e no padrão obrigatório (Homologação da ICP -Brasil NSH-2 ou NSH-3) conforme observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP -BRASIL [9].

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7 Propósito de uso de chave (Conforme o campo “key usage” NA X. 509 V3)

6.1.7.1. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC CNDL RFB, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC implementada.

6.1.7.2. Os pares de chaves correspondentes aos certificados emitidos pela AC CNDL RFB podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do

não repúdio e para cifragem de chaves. Para isso, os certificados emitidos pela AC CNDL RFB têm ativados os bits DigitalSignature, NonRepudiation e KeyEncipherment.

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

A AC CNDL RFB implementa uma combinação de controles físicos (item 5.1.2), lógicos e procedimentais (item 5.2), de forma a garantir a segurança de suas chaves privadas. As chaves privadas da AC CNDL RFB são armazenadas de forma cifrada nos mesmos componentes seguros de hardware utilizados para sua geração. O acesso a esses componentes é controlado por meio de chave criptográfica de ativação. Os titulares de certificados emitidos pela AC CNDL RFB, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado das suas chaves privadas.

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC CNDL RFB adota o padrão FIPS (Federal Information Processing Standards) 140-2, nível 3 (para as cadeias de certificação V2 e V5), conforme observado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas possui certificação INMETRO]. Cada PC implementada especifica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.2.2 Controle de “N de M” para chave privada

6.2.2.1. Para a utilização das suas chaves privadas, a AC CNDL RFB define a forma de controle múltiplo, do tipo “n” pessoas de um grupo de “m”.

6.2.2.2. A AC CNDL RFB estabelece como exigência de controle múltiplo para a utilização das suas chaves privadas: número mínimo de 2 ("n") (duas) pessoas de um grupo de 8 ("m") (oito) pessoas para utilização das suas chaves privadas.

6.2.3 Custódia (Escrow) de chave privada

Não é permitida, no âmbito ICP Brasil, a custódia (Escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

A AC CNDL não implementa a recuperação de chaves privadas.

6.2.4 Cópia de Segurança de chave privada

6.2.4.1. Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC CNDL RFB mantém cópia de segurança de sua própria chave privada.

6.2.4.3. A AC CNDL RFB não mantém cópia de segurança de chave privada de titular de certificados e -CPF e e-CNPJ por ela emitido.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1. A AC CNDL RFB arquiva chaves privadas de assinatura de titulares de certificados.

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

6.2.6 Inserção de chave privada em módulo criptográfico

6.2.6.1. A AC CNDL RFB gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1

6.2.8 Método de ativação de chave privada

6.2.8.1. Para a ativação das chaves privadas a AC CNDL RFB exige o número mínimo de 2 ("n") (dois) detentores de chaves criptográficas de um grupo de 8 ("m") (oito) conforme perfil qualificado.

6.2.8.2. A confirmação da identidade desses agentes é feita através da utilização das suas respectivas partições e de suas senhas, com logon no módulo criptográfico e ativação da chave da AC CNDL. Só lhes é permitido o acesso ao ambiente, em duplas devidamente autorizadas. Essas pessoas são identificadas pelo crachá funcional contendo fotografia, nome, e departamento do funcionário.

Cada PC implementada pela AC CNDL RFB descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

6.2.9 Método de desativação de chave privada

A chave privada da AC CNDL RFB, só permite o acesso em duplas devidamente autorizadas pelo sistema de controle de acesso da AC CNDL RFB. Somente as pessoas qualificadas, após a sua devida identificação e autorização feita através da ativação de seus equipamentos criptográficos, da utilização de suas partições e senhas, têm acesso ao sistema de certificação, onde são executados os comandos de logoff, desativando a chave privada da AC CNDL RFB. Essas pessoas são identificadas pelo crachá funcional contendo fotografia, nome, e departamento do funcionário.
Cada PC implementada pela AC CNDL RFB descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.10 Método de destruição de chave privada

Para a destruição das chaves privadas a AC CNDL RFB exige o número mínimo de 2 ("n") (dois) detentores de chaves criptográficas um grupo de 8 ("m") (oito) conforme perfil qualificado. A confirmação da identidade desses detentores é feita através de crachás e senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

As mídias de armazenamento das chaves privadas são reinicializadas de forma a não restarem nelas informações sensíveis.

Cada PC implementada pela AC CNDL RFB descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública

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

6.3.2 Períodos de operação do certificado e períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas da AC CNDL RFB e dos titulares de certificados de assinatura digital por ela emitidos, são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas bem como as LCR´S emitidas pela AC CNDL RFB podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Item não aplicável.

6.3.2.3. Cada PC implementada pela AC CNDL RFB define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.4. A validade admitida para certificados da AC CNDL RFB é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4 DADOS DE ATIVAÇÃO

6.4.1 Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação do equipamento de criptografia que armazena a chave privada da AC CNDL RFB são únicos e aleatórios.

6.4.1.2. Cada PC implementada pela AC CNDL RFB garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão únicos e aleatórios.

6.4.2 Proteção dos dados de ativação

6.4.2.1. Os dados de ativação da chave privada da AC CNDL RFB são protegidos contra uso não autorizado, por meio de mecanismos de criptografia e de controle de acesso físico.

6.4.2.2. Cada PC implementada pela AC CNDL RFB garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

6.4.3 Outros aspectos do dado de ativação

Item não aplicável

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1. A geração do par de chaves da AC CNDL RFB é realizada off-line, para impedir o acesso remoto não autorizado.

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

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

6.5.1.2. Os requisitos específicos aplicáveis são descritos em cada PC da AC CNDL RFB implementada.

6.5.1.3. Cada computador servidor da AC CNDL RFB, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) Controle de acesso aos serviços e perfis da AC CNDL RFB;

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

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

d) Geração e armazenamento de registros de auditoria da AC CNDL RFB;

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

f) Mecanismos para cópias de segurança (backup).

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

6.5.1.5. Qualquer equipamento ou parte deste ao ser enviado para manutenção, tem apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC CNDL RFB, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixa de ser utilizado em caráter permanente, serão destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC CNDL RFB. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC CNDL RFB é preparado e configurado como previsto na Política de Segurança implementada, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2 Classificação da segurança computacional

A segurança computacional da AC CNDL RFB segue as recomendações do Trusted System Evaluation Criteria (TCSEC).

6.5.3 Controles de segurança para autoridades de registro

6.5.3.1. 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.

6.5.3.2. São incluídos, no mínimo, os requisitos especificados em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR´S da ICP-Brasil.

6.5.3.2.1. As partições 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.

6.5.3.2.2. As estações de trabalho das AR`S vinculadas a AC CNDL RFB implementam aplicação e faz o controle de integridade das configurações da aplicação de AR, bem como dos arquivos de configuração ou informações críticas mantidas na estação de trabalho.

6.5.3.2.3. As estações de trabalho das AR`S vinculadas a AC CNDL RFB contém apenas aplicações e serviços que são suficientes e necessários para as atividades corporativas.

6.5.3.2.4. As estações de trabalho das AR´S vinculadas a AC CNDL RFB, 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 registrodurante 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.

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

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

6.5.3.2.7. Os Agentes de Registro das AR´S vinculadas à AC CNDL RFB, não possuem perfil de administrador ou senha de *root* dos equipamentos ou com privilégios especiais do sistema, ficando essa tarefa delegada a outros da própria organização, para permitir segregação de funções. O Agente de Registro recebe acesso somente aos serviços e aplicações que tenham sido especificamente autorizados a usar.

6.5.3.2.8. O aplicativo que faz interface entre as AR`S vinculadas e o sistema de certificação da AC CNDL RFB possuem 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.

6.5.3.2.9. O aplicativo das Autoridades de Registro vinculadas a AR CNDL RFB:

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

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

6.5.3.3. Item não aplicável.

6.6 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.

6.6.1 Controles de desenvolvimento de sistema

6.6.1.1. 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.

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

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. 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.

Caso haja divergência, são tomadas medidas adequadas para a recuperação da situação, levando-se em consideração a natureza do problema e a análise do fato gerador, para evitar a sua recorrência.

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

6.6.3 Controles de segurança do ciclo de vida

Item não aplicável.

6.6.4 Controles na geração de LCR

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

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 Diretrizes gerais

6.7.1.1. Abaixo são descritos os controles relativos à segurança da rede da AC CNDL RFB, incluindo firewalls e recursos similares.

6.7.1.2. Nos servidores do sistema de certificação da AC CNDL RFB, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

6.7.1.3. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC CNDL RFB, estão localizados e operam em ambiente de nível 4.

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

6.7.1.5. O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectadosa redes externas implementamfiltros de pacotes de dados, que permitem somente as conexões aos serviços e servidorespreviamente definidos como passíveis de acesso externo.

6.7.2 Firewall

6.7.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função na AC CNDL RFB. Firewalls promovem o isolamento, em subredes específicas, dos equipamentos servidores com acesso externo - a conhecida "zona desmilitarizada" (DMZ) - em relação aos equipamentos com acesso exclusivamente interno à AC CNDL RFB.

6.7.2.2. O firewall utilizado pela AC CDNL RFB, entre outras características, provê registros dos eventos em logs, além de implementar uma gerência de configuração.

6.7.3 Sistema de detecção de intrusão (IDS)

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

6.7.3.2. O sistema de detecção de intrusão da AC CNDL RFB, tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base em tempo real.

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

6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado - em roteadores, firewalls ou IDS na AC CNDL RFB, são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é, no mínimo, diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 CARIMBO DO TEMPO

Item não aplicável.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 PERFIL DO CERTIFICADO

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

7.1.1 Número (s) de versão

Todos os certificados emitidos pela AC CNDL RFB implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões do certificado

Item não aplicável.

7.1.3 Identificadores de Algoritmo

Item não aplicável.

7.1.4 Formatos de nome

Item não aplicável.

7.1.5 Restrições de nome

Item não aplicável.

7.1.6 OID (Object Identifier) de DPC

O OID desta DPC-AC CNDL RFB é 2.16.72.1.1.65.

7.1.7 Uso da extensão “POLICY CONSTRAINSTS”

Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Item não aplicável.

7.1.9 Semântica de processamento para extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 PERFIL DE LCR

7.2.1 Número (s) de versão

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

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1. Abaixo são descritas todas as extensões de LCR´S utilizadas pela AC CNDL RFB e sua criticidade.

7.2.2.2. As LCR´S da AC CNDL RFB e SRF obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

a) "Authority Key Identifier" não crítica: contém o hash SHA-1 da chave pública da AC CNDL RFB e;

b) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC CNDL RFB;

7.3 PERFIL DE OCSP

7.3.1 Número (s) de versão

Item não aplicável.

7.3.2 Extensões de OCSP

Item não aplicável.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 FREQUÊNCIA E CIRCUNSTÂNCIA 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.

8.2 IDENTIFICAÇÃO/ QUALIFICAÇÃO DO AVALIADOR

8.2.1 As fiscalizações das entidades da AC CNDL RFB integrantes da ICP Brasil, são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP - BRASIL [2].

8.2.2. Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP -Brasil, as auditorias das entidades integrantes da AC CNDL RFB são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP -BRASIL [3].

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

As auditorias das entidades da AC CNDL RFB integrantes da ICP Brasil, são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARAREALIZAÇÃO DE AUDITORIAS NASENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.4.1 As fiscalizações e auditorias das entidades da AC CNDL RFB, realizadas no âmbito da ICP -Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades da AC CNDL RFB estão em conformidade com suas respectivas DPC, PC´S, PS´S e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *Web Trust.*

8.4.2. 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.

8.4.3. 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.

8.5 AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

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

8.6 COMUNICAÇÃO DOS RESULTADOS

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

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 TARIFAS

9.1.1 Tarifas de emissão e renovação de certificados

Variável conforme definição interna comercial.

9.1.2 Tarifa de acesso ao certificado

A AC CNDL RFB não cobra tarifas de acesso ao certificado digital emitido.

9.1.3 Tarifa de revogação ou acesso à informação de status

Na AC CNDL RFB não há tarifa de revogação ou de acesso à informação de status de certificado.

9.1.4 Tarifa para outros serviços

A AC CNDL RFB não cobra 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 RESPONSABILIDADE FINANCEIRA

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

9.2.1 Cobertura de seguro

Conforme item 4 desta DPC.

9.2.2 Outros ativos

Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para entidades finais

A AC CNDL RFB implementa uma política que contém informações sobre a utilização correta da garantia oferecida sobre os seus certificados digitais, cartões inteligentes, tokens e as leitoras de cartão inteligente, e está de acordo com a legislação vigente, especialmente, o Código de Defesa do Consumidor (CDC).

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 Escopo de informações confidenciais

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

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

9.3.2 Informações fora do escopo de informações confidenciais

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

a) os certificados e as LCR´S 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.

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

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

a) qualquer PC aplicável;

b) qualquer DPC;

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

d) a conclusão dos relatórios da auditoria.

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

9.3.3 Responsabilidade em proteger a informação confidencial

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

9.3.3.2 A chave privada de assinatura digital da AC CNDL RFB é gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC CNDL RFB é de sua inteira responsabilidade.

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

9.3.3.4 Item não aplicável.

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1 Plano de privacidade

A AC CNDL RFB assegura a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2 Tratamento de informações como privadas

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

9.4.3 Informações não consideradas privadas

Informações sobre revogação de certificados de usuários finais são fornecidas na LCR da AC CNDL RFB.

9.4.4 Responsabilidade para proteger a informação privada

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

9.4.5 Aviso e consentimento para utilizar informações privadas

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

9.4.5.2. O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

9.4.5.3. Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou

b) por meio de pedido escrito com firma reconhecida.

9.4.6 Divulgação em processo judicial ou administrativo

9.4.6.1. Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC CNDL RFB será fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

9.4.6.2. As informações privadas ou confidenciais sob a guarda da AC CNDL RFB poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7 Outras circunstâncias de divulgação de informação

Item não aplicável.

9.4.8 Informações a terceiros

Nenhum documento, informação ou registro sob a guarda das AR´S vinculadas 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 DIREITO DE PROPRIEDADE INTELECTUAL

De acordo com a legislação vigente.

9.6 DECLARAÇÕES E GARANTIAS

9.6.1 Declarações e garantias da AC

A AC CNDL RFB declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

A AC CNDL RFB implementa procedimentos para verificar a autorização da emissão de um certificado ICP - Brasil, contidas nos itens 3 e 4 desta DPC. A AC CNDL RFB, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das AR na forma de sua DPC, PC´S e normas complementares.

9.6.1.2 Precisão da informação

A AC CNDL RFB implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC Raiz, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das AC´S s subsequentes e AR na forma de sua DPC, PC´S e normas complementares.

9.6.1.3 Identificação do requerente

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

9.6.1.4 Consentimento dos titulares

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

9.6.1.5 Serviço

A AC CNDL RFB mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios e LCR´S.

9.6.1.6 Revogação

A AC CNDL RFB revogará certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil.

9.6.1.7 Existência Legal

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

9.6.2 Declarações e garantias da AR

Em acordo com item 4 desta DPC.

9.6.3 Declarações e garantias do titular

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

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

9.6.4 Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes devem:

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

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

9.6.4.2. Item não aplicável.

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

9.6.5 Representação e garantias de outros participantes

Item não aplicável.

9.7 ISENÇÃO DE GARANTIAS

Item não aplicável.

9.8 LIMITAÇÕES DE RESPONSABILIDADES

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

9.9 INDENIZAÇÕES

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

9.10 PRAZO E RESCISÃO

9.10.1 Prazo

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

9.10.2 Término

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

9.10.3 Efeito da rescisão e sobrevivência

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

9.11 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

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

9.12 ALTERAÇÕES

9.12.1 Procedimentos para emendas

Qualquer alteração nesta DPC será submetida para AC RFB e AC Raiz.

9.12.2 Mecanismo de notificação e período

Mudança nesta DPC será publicado no site da AC CNDL RFB.

9.12.3 Circunstância na qual o OID deve ser alterado

Item não aplicável.

9.13 SOLUÇÃO DE CONFLITOS

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

9.13.2. A DPC da AC CNDL RFB não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14 LEI APLICÁVEL

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

9.15 CONFORMIDADE COM A LEI APLICÁVEL

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

9.16 DISPOSIÇÕES DIVERSAS

9.16.1 Acordo completo

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

9.16.2 Cessão

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

9.16.3 Independência de disposições

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

9.16.4 Execução (Honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17 OUTRAS PROVISÕES

Item não aplicável.

10 DOCUMENTOS REFERENCIADOS

10.1 RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-BRASIL

Os documentos abaixo são aprovados por Resoluçõesdo 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
[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
[9]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORES DA ICP-BRASIL	DOC-ICP-05

[1]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

10.2 APROVAÇÕES DA AC RAIZ

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

Ref.	Nome do documento	Código
[4]	TERMOS DE TITULARIDADE	ADE-ICP-05. B

10.3 APROVAÇÕES DA AC RFB

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

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

11 REFERÊNCIAS BIBLIOGRÁFICAS

[5] WebTrust Principles and Criteria for Registration Authorities, disponível em: https://www.webtrust.org/

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

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

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

RFC 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, september 2007

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

RFC 6712, IETF - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.