DOCCLOUD
CERTIFICADO DIGITAL

Declaração de Práticas de Certificação da AC DOCCLOUD RFB
DPC da AC DOCCLOUD RFB

OID: 2.16.76.1.1.71
Versão 7.0

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

CONTROLE DE ALTERAÇÕES

RESPONSÁVEL	APROVAÇÃO	DESCRIÇÃO DA ALTEAÇÃO	VERSÃO	DATA
Compliance	Resolução nº 204, de 16.11.2022	Conforme recomendações da resolução supracitada.	7.0	22.12.2022
Compliance	Resolução nº 197, de 16.11.2021 Versão 6.2	Regulamentação dos procedimentos e requisitos técnicos para a operacionalização de Autoridade de Registro Eletrônica na ICP-Brasil.	6.0	17.08.2022
Compliance		Informações administrativas da AC DOCCLOUD RFB	5.1	01.09.2021
Compliance	Resoluções 177/2020 e 181/2021	Regulamenta a emissão de certificado digital de pessoa física de forma conjunta com Carteira de Identidade (RG) e Carteira Nacional de Habilitação (CNH) e a emissão de certificado digital de pessoa jurídica pelas juntas comerciais. Inclui a previsão de batimento biométrico e biográfico, realizado em base oficial nacional, no processo de identificação de requerente de certificado digital ICP-Brasil.	5.0	26.02.2021
Compliance	Instruções Normativas 02 e 03 de 2020	Solicitação de Certificado Digital por videoconferência e Procedimentos para aprovação de normativos da AC.	4.0	08.05.2020
Compliance	Resolução 151 e 154 - 2019	Atualização dos requisitos Webtrust e consolidação com a versão 4.7, com a simplificação dos processos da ICP-Brasil. Estender a etapa de verificação para AR de PSS da AC.	3.0	21.10.2019
Compliance		Atualização das Informações de contato da AC.	2.1	05.12.2018
Compliance	Resolução 130 - 2017	Procedimentos de validação fora do ambiente físico da AR.	2.0	29.08.2018
Compliance	Resolução 119 - 2017	Obrigatoriedade de realização de auditorias WebTrust e de implementação de respostas OCSP para certificados do tipo SSL/TLS.	2.0	29.08.2018

Compliance	IN nº 07 - 2016	conformidade aos requisitos do programa de raízes confiáveis para manutenção dos certificados da AC RAIZ da ICP-Brasil nos repositórios dos navegadores de internet.	2.0	29.08.2018
Compliance	Resolução 116 - 2015	Referência à autoridade certificadora Raiz V5 e suas cadeias subsequentes.	2.0	29.08.2018
Compliance	Versão Inicial		1.0	12.06.2015

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora DOCCLOUD para a Secretaria da Receita Federal do Brasil - AC DOCCLOUD RFB integrante na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços de certificação digital.

1.1.2. Esta Declaração de Práticas de Certificação – DPC, adota obrigatoriamente a estrutura e requisitos empregados pelo documento: Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil – DOC-ICP-05, em sua versão 6.1.

1.1.3 Item não aplicável.

1.1.4. A estrutura desta DPC da AC DOCCLOUD RFB está baseada nas resoluções do Comitê Gestor da ICP-Brasil (CG ICP-Brasil) e na RFC 3647.

1.1.5. A AC DOCCLOUD RFB mantém atualizada esta Declaração de Práticas de Certificação de acordo com as resoluções do Comitê Gestor da ICP-Brasil.

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. Este documento é chamado “Declaração de Práticas de Certificação da Autoridade Certificadora DOCCLOUD” e comumente referido como “DPC da AC DOCCLOUD RFB”. O Identificador de Objeto **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.71.**

1.2.2. A AC DOCCLOUD RFB emissora de certificados para usuários finais é exclusiva e separada de acordo com o propósito de uso de chaves de Assinatura de documento e proteção de e-mail (S/MIME).

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. Autoridades Certificadoras

Esta DPC refere-se unicamente à Autoridade Certificadora DOCCLOUD RFB - AC DOCCLOUD RFB e encontra-se publicada no seu repositório, no seguinte endereço: doccloud.com.br/repositorios/acdoccloudrfb

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC DOCCLOUD RFB para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da doccloud.com.br/repositorios/acdoccloudrfb com a seguintes informações:

a) relação de todas as AR credenciadas;
b) relação de AR que tenham se descredenciado da cadeia da AC DOCCLOUD RFB, com respectiva data do descredenciamento;

1.3.3. Titulares de Certificado

Pessoas físicas ou jurídicas inscritas no CPF ou no CNPJ podem ser Titulares de Certificado e-CPF ou e-CNPJ Tipo A1 e A3, desde que não enquadradas na situação cadastral de CANCELADA ou NULA (pessoa física) ou na condição de BAIXADA, INAPTA, SUSPENSA ou NULA (pessoa jurídica), 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).

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

1.3.5. Outros Participantes
Os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviços de Confiança - PSC vinculados à AC DOCCLOUD RFB estão relacionados em sua página web doccloud.com.br/repositorios/acdoccloudrfb

1.3.5.1 PSS, PSBios ou PSC são entidades utilizadas pela AC DOCCLOUD RFB ou pelas ARs vinculadas para desempenhar atividade descrita nesta DPC ou na PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.4. USABILIDADE DO CERTIFICADO

1.4.1. Uso apropriado do certificado
A AC DOCCLOUD RFB implementa as seguintes Políticas de Certificado Digital:

Para Certificados de Assinatura Digital:

POLÍTICA DE CERTIFICADO	NOME	OID
Política de Certificado de Assinatura Digital do tipo A1 da AC DOCCLOUD RFB	*PC A1 da AC DOCCLOUD RFB*	*2.16.76.1.2.1.58*
Política de Certificado de Assinatura Digital do tipo A3 da AC DOCCLOUD RFB	*PC A3 da AC DOCCLOUD RFB*	*2.16.76.1.2.3.55*

Nas PC correspondentes estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC DOCCLOUD RFB e, quando cabíveis, as aplicações para as quais existem restrições ou proibições para o uso desses certificados.

1.4.2. Uso proibitivo do certificado
Quando cabível, as aplicações para as quais existam restrições ou proibições para o uso desses certificados estão listados nas PCs implementadas.

1.5. POLÍTICA DE ADMINISTRAÇÃO

Neste item estão incluídos nome, endereço e outras informações da AC DOCCLOUD RFB, assim como são informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1. Organização administrativa do documento
AC DOCCLOUD RFB
DOCCLOUD SOLUCAO DIGITAL

1.5.2. Contatos
Endereço: Rua Gonçalves Dias, 519 – Jardim Girassol - Americana/SP - CEP: 13.465-670.
Telefone: (19) 3477-1144
Página Web: www.doccloud.com.br

1.5.3. Adequabilidade das DPC's com PC's

AC DOCCLOUD RFB

Nome: Lucas Carvalho dos Santos
Departamento: NORMAS & COMPLIANCE
Telefone: (19) 3477-1144
E-mail: compliance@doccloud.com.br

1.5.4. Procedimentos de aprovação desta DPC

Este documento foi analisado pela alta gestão da AC DOCCLOUD RFB e submetido ao Instituto de Tecnologia da Informação – ITI para aprovação. Os procedimentos de aprovação da DPC da AC DOCCLOUD RFB são estabelecidos a critério do CG da ICP-Brasil.

1.6. DEFINIÇÕES E ACRÔNICOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
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
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
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	Prestador de Serviço de Suporte
PUK	PIN Unbloking Key
RFC	Request For Comments
RG	Registro Geral
SIGEPE	Sistema de Gestão de Pessoal da Administração Pública Federal
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TLS	Transport Layer Security
TSDM	Trusted Software Development Methodology
TSE	Tribunal Superior Eleitoral

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. REPOSITÓRIOS

2.1.1. O repositório da AC DOCCLOUD RFB é mantido em ambiente próprio e possui recursos físicos, humanos e de infraestrutura computacional aptos a:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC DOCCLOUD RFB e a sua LCR;

b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e

c) implementar os recursos necessários para a segurança dos dados nele armazenados.

2.1.2. As publicações da AC DOCCLOUD RFB podem ser consultadas através do protocolo http, onde somente a AC DOCCLOUD RFB, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas no seu repositório.

2.1.3. O repositório da AC DOCCLOUD RFB está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e pode ser encontrado na página Web doccloud.com.br/repositorios/acdoccloudrfb

2.1.4 A AC DOCCLOUD RFB disponibiliza 2 (dois) repositórios em infraestrutura de rede segregadas para distribuição de LCR/OCSP, nos endereços:

a) Para Certificados da Cadeia V2:
http://repositorio.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv2.crl
http://repositorio2.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv2.crl

b) Para Certificados da Cadeia V5:
http://repositorio.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv5.crl
http://repositorio2.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv5.crl

2.2. PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICADOS

2.2.1. A AC DOCCLOUD RFB pública e disponibiliza informações, tais como certificados, LCR, sua DPC, entre outras, em página WEB, com disponibilidade 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 são publicadas na página web da AC DOCCLOUD RFB em: doccloud.com.br/repositorios/acdoccloudrfb

a) o certificado da AC DOCCLOUD RFB;
b) suas LCR's e/ou OCSP;

c) sua DPC;
d) as PC's que implementa;
e) relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços;
f) relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.3.1. De modo a assegurar a disponibilização sempre atualizada de seus conteúdos:

a) os certificados são publicados imediatamente após sua emissão;
b) a publicação da LCR se dá conforme o item 4.9.7 desta DPC;
c) as versões ou alterações desta DPC são atualizadas no web site da AC DOCCLOUD RFB após aprovação da AC Raiz da ICP-Brasil; e
d) os endereços das AR vinculadas são atualizadas no web site da AC DOCCLOUD RFB

2.4. CONTROLE DE ACESSO AOS REPOSITÓRIOS

2.4.1. Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC DOCCLOUD RFB e aos endereços das AR vinculadas.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. ATRIBUIÇÕES DE NOMES

3.1.1. Tipos de nomes

3.1.1.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "distinguished name" do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular.

3.1.1.2. Item não aplicável.

3.1.2. Necessidade de nomes serem significativos

3.1.2.1. Os certificados emitidos pela AC DOCCLOUD RFB exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da pessoa ou da organização titular do certificado.

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

Item não aplicável.

3.1.4. Regras para interpretação de vários tipos de 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. Unicidades de nomes

Esta DPC estabelece que identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado emitido pela AC DOCCLOUD RFB.

Para assegurar a unicidade do campo dos certificados e-CNPJ e e-CPF é incluído o número do CNPJ e o número do CPF após o nome do titular do certificado, respectivamente, nos certificados e-CNPJ e e-CPF.

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

A AC DOCCLOUD RFB se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrentes da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas
Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

3.2. VALIDAÇÃO INICIAL DE IDENTIDADE

Neste item e nos itens seguintes estão descritos em detalhe os requisitos e procedimentos utilizados pelas AR vinculadas à AC DOCCLOUD RFB para a 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 e 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 biometrias apresentadas, vedada qualquer espécie de procuração para tal fim.
>
> ii. para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.

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

3.2.1. Método para comprovar o controle de chave privada
A AR's vinculadas à AC DOCCLOUD RFB verifica 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.

No caso em que sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos são descritos nessas PCs, no item correspondente.

3.2.2. Autenticação da identidade de uma organização

3.2.2.1. Disposições Gerais
3.2.2.1.1. A confirmação da identidade de uma pessoa jurídica é feita mediante consulta aos dados fornecidos pela RFB.

3.2.2.1.2. Em sendo o titular do certificado pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo

responsável pela pessoa jurídica cadastrado no CNPJ da RFB.

3.2.2.1.3. A AC DOCCLOUD RFB realiza a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) apresentação do rol de documentos elencado no item 3.2.2.2;
b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
c) coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil, bem como os procedimentos para identificação biométrica na ICP-Brasil; e
d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo titular ou responsável pelo uso do certificado.

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

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

3.2.2.1.5. O disposto no item 3.2.2.1.3 poderá ser realizado:

a) mediante comparecimento presencial do responsável pelo certificado; ou

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

3.2.2.2. Documentos para efeitos de identificação de uma organização
A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos à sua habilitação jurídica:

i. se pessoa jurídica cuja criação se deu ou foi autorizada por lei, cópia do ato constitutivo e CNPJ;

ii. se entidade privada:
1) Ato constitutivo, devidamente registrado no órgão competente ou Certidão Simplificada da Junta Comercial do seu registro; 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 um indivíduo
3.2.2.3.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;
b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
c) Nome completo do responsável pelo certificado, sem abreviações; e
d) Data de nascimento do responsável pelo certificado.

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

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

3.2.3. Autenticação da identidade de um indivíduo
A confirmação da identidade de um indivíduo é realizada mediante a presença física ou por um dos procedimentos listados nas alíneas abaixo, com nível de segurança equivalente e observado pelas normas técnicas da ICP-Brasil do interessado, com base em documentos pessoais de identificação legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil:

a) Item não aplicável;
b) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz; e
c) item não aplicável.

3.2.3.1. Procedimento 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 ou digital:

i. Registro de Identidade, se brasileiro; ou
ii. Título de Eleitor, com foto; ou
iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
iv. Passaporte, se estrangeiro não domiciliado no Brasil.

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

NOTA 01: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

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 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 à etapa de identificação;
b) na sede da AR ou AR própria 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) nome completo, sem abreviações;
b) data de nascimento; e
c) Cadastro da Pessoa Física (CPF).

3.2.3.2.1.1 Item não aplicável.

3.2.3.2.2 Cada PC da AC DOCCLOUD RFB define 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 Específico do INSS (CEI);
d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;
e) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente; e
f) documento assinado pela empresa com o valor do campo de login (UPN).

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

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

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

3.2.3.2.3.1 Item não aplicável.

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

3.2.7.1 Disposições Gerais
Item não aplicável.

3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação
Item não aplicável.

3.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação
Item não aplicável.

3.2.7.4 Autenticação de identificação de equipamento para certificado CF-e-SAT
Item não aplicável.

3.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT
Item não aplicável.

3.2.7.6 Informações contidas no certificado emitido para um equipamento SAT
Item não aplicável.

3.2.7.7 Autenticação de identificação de equipamentos para certificado OM-BR

3.2.7.7.1 Disposições gerais
Item não aplicável.

3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico
Item não aplicável.

3.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico
Item não aplicável.

3.2.8 Procedimentos complementares
3.2.8.1 A AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro.

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

3.2.8.2.1 Item não aplicável.

3.2.8.3 Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias são mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

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 disponibiliza, para todas as AR 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 DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

3.2.8.4.1 Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, fica 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
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
No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC DOCCLOUD RFB para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

3.3.2. Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

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

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

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

d) solicitação por meio eletrônico dada nas alíneas ‘b’ e ‘c’, acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação 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 na PC implementada.

3.3.4. Item não aplicável.

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante.

A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas. O procedimento para solicitação de revogação de certificado emitido pela AC DOCCLOUD RFB está descrito no item 4.9.3.

Solicitações de revogação de certificados devem ser registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 Solicitação do certificado

4.1.1. Neste item são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC DOCCLOUD RFB e pelas ARs a ela vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos compreendem todas as ações necessárias tanto do indivíduo solicitante quanto das AC e AR no processo de solicitação de certificado digital e contemplam:

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

b) o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; ou quando da emissão para servidores públicos da ativa e militares da União, Estados e Distrito Federal, por servidor público e militar autorizado pelos sistemas de gestão de pessoal dos órgãos competentes;

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

d) Item não aplicável.

A AC DOCCLOUD RFB adequou o sistema para atendimento a essa modalidade, seguindo requisitos descrito no DOC-ICP-05.05. Assim sendo, os futuros e/ou titulares deverão atender no mínimo os requisitos descritos acima para ter o acesso à emissão do certificado através de videoconferência

> **NOTA 1**: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados de equipamento ou outros que façam uso de CSR) 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

A submissão da solicitação deve ser sempre por intermédio da AR.

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

Abaixo são descritas as obrigações gerais das entidades envolvidas. Não existem procedimentos específicos na PC implementada.

4.1.2.1 Responsabilidades da AC

4.1.2.1.1 A AC DOCCLOUD RFB responde pelos danos a que der causa.

4.1.2.1.2 A AC DOCCLOUD RFB responde solidariamente pelos atos das entidades de sua cadeia de certificação AR e PSS.

4.1.2.1.3 Item não aplicável.

4.1.2.2 Obrigações da AC DOCCLOUD RFB

As obrigações da AC DOCCLOUD RFB são as abaixo relacionadas:

a) operar de acordo com a sua DPC e com as PCs que implementa;
b) gerar e gerenciar os seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar à AC RFB de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar à imediata revogação do correspondente certificado;
e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AR a ela vinculadas e de usuários finais;
h) informar à emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - On-line Certificate Status Protocol);
k) publicar em sua página web sua DPC e as PCs aprovadas que implementa;
l) publicar, em sua página web, as informações definidas no item 2.2.2 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 à integridade, o sigilo e a segurança da informação por ela tratada;
s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada à AC DOUCLOUD RFB
y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados

4.1.2.3 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

4.1.2.4 As obrigações das AR's

As obrigações das ARs vinculadas à AC DOCCLOUD RFB são as 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 DOCCLOUD RFB utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICPBRASIL [1];
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 ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], bem como Princípios e Critérios WebTrust para AR [14];
f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2, 3.2.3; e
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 [14].

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1 Execução das funções de identificação e autenticação
A AC e AR executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2 Aprovação ou rejeição de pedidos de certificado
Item não aplicável.

4.2.3 Tempo para processar a solicitação de certificado
À AC DOCCLOUD 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 DOCCLOUD RFB durante à emissão de um certificado
4.3.1.1 A emissão de certificado depende do correto preenchimento de formulário de solicitação, da assinatura do "Termo de Titularidade", no caso de certificados de pessoas jurídicas, ou aplicações e dos demais documentos exigidos. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e Titular é notificado da emissão e do método para a retirada do certificado.

4.3.1.2 O certificado é considerado válido a partir do momento de sua emissão.

4.3.2 Notificações para o titular do certificado pela AC DOCCLOUD RFB na emissão do certificado
O Titular é notificado da emissão e do método para a retirada do certificado.

4.4 ACEITAÇÃO DE CERTIFICADO

4.4.1 Conduta sobre a aceitação do certificado
4.4.1.1 O titular do certificado ou pessoa física responsável verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

a) concorda com as responsabilidades, obrigações e deveres nesta DPC;
b) garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.1.2 A AC DOCCLOUD RFB garante que a aceitação de todo certificado emitido seja declarada pelo respectivo

titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

4.4.1.3 Eventuais termos de acordo, ou instrumentos similares, se necessários, são descritos neste item da PC correspondente.

4.4.2 Publicação do certificado pela AC DOCCLOUD RFB
Os certificados da AC DOCCLOUD RFB são publicados 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 da DPC da AC Raiz.

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

A AC DOCCLOUD RFB e o titular do certificado para usuário final devem operar de acordo com a esta 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
Eventuais termos de acordo, ou instrumentos similares, se necessários, são descritos neste item da PC correspondente.

4.5.1.2 Obrigações do Titular do Certificado.

As obrigações dos titulares de certificados emitidos de acordo com esta DPC da AC DOCCLOUD RFB são as abaixo relacionadas:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, código de ativação (PIN) e dispositivos criptográficos;
c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e
e) informar à AC DOCCLOUD RFB qualquer comprometimento de 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 uso do certificado.

4.5.2 Usabilidade da chave pública e do certificado 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 de 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
Item não aplicável

4.6.7 Notificação de emissão de certificado pela AC para outras entidades
Em acordo com item 4.3 desta DPC.

4.7 NOVA CHAVE DE CERTIFICADO (Re-key)

4.7.1 Circunstâncias para nova chave de certificado
Item não aplicável

4.7.2 Quem pode requisitar a certificação de uma nova chave pública
Item não aplicável

4.7.3 Processamento de requisição de novas chaves de certificado
Item não aplicável

4.7.4 Notificação de emissão de novo certificado para o titular
Item não aplicável

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada
Item não aplicável

4.7.6 Publicação de uma nova chave certificada pela AC
Item não aplicável

4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades
Item não aplicável

4.8 MODIFICAÇÃO DE CERTIFICADO
Item não aplicável

4.8.1 Circunstâncias para modificação de certificado
Item não aplicável

4.8.2 Quem pode requisitar a modificação de certificado
Item não aplicável

4.8.3 Processamento de requisição de modificação de certificado
Item não aplicável

4.8.4 Notificação de emissão de novo certificado para o titular
Item não aplicável

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado
Item não aplicável

4.8.6 Publicação de uma modificação de certificado pela AC
Item não aplicável

4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades
Item não aplicável

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1 Circunstâncias para revogação

4.9.1.1. O titular do certificado pode solicitar a revogação do seu certificado em qualquer altura e independentemente de qualquer circunstância.

4.9.1.2. Um certificado é obrigatoriamente revogado:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;
b) Quando for necessária a alteração de qualquer informação constante no mesmo;
c) Item não aplicável; e
d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3 Este DPC observa ainda que:

a) A AC DOCCLOUD 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; e

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

4.9.1.4 Todo certificado tem a sua validade verificada, na respectiva LCR ou OCSP, 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 DOCCLOUD RFB e do período de validade da LCR.

4.9.2 Quem pode solicitar revogação
A DPC estabelece que a revogação de um certificado somente poderá ser feita:

a) Por solicitação do titular do certificado;
b) Por solicitação do responsável pelo certificado, no caso de pessoas jurídicas;
c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
d) Pela AC DOCCLOUD RFB;
e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
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. É necessária uma solicitação de revogação para que AR responsável inicie o processo de revogação. As instruções para a solicitação de revogação do Certificado são obtidas em página web disponibilizada pela AC DOCCLOUD RFB ou pela AR Responsável.

A revogação é realizada através de formulário contendo o motivo da solicitação de revogação e mediante o fornecimento de dados indicados na solicitação de emissão do certificado, ou por formulário assinado pelo titular na falta desses dados.

4.9.3.2. Como diretrizes gerais, fica estabelecido que:

a) o solicitante da revogação de um certificado será identificado;

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

c) as justificativas para a revogação de um certificado serão documentadas; e

d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado, e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado na base de dados da AC DOCCLOUD RFB, quando aplicável.

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

4.9.3.4 Item não aplicável;

4.9.3.5 A AC DOCCLOUD RFB responsável responderá plenamente por todos os danos causados pelo uso do 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 4.4.1. O prazo para aceitação do certificado pelo titular é de 2 (dois) dias úteis, dentro desse prazo a revogação do certificado pode ser solicitada sem ônus.

4.9.4.2. Item não aplicável.

4.9.5 Tempo em que a AC deve processar o pedido de revogação

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

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7 Frequência de emissão de LCR

4.9.7.1. Neste item é definida a frequência para a emissão de LCR da AC DOCCLOUD RFB.

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

A AC DOCCLOUD RFB não disponibiliza recursos para revogação on-line de certificados.

4.9.10 Requisitos para verificação de revogação on-line
Item não aplicável.

4.9.11 Outras formas disponíveis para divulgação de revogação
4.9.11.1 Além das LCRs, a AC DOCCLOUD RFB poderá utilizar outros meios para divulgação de informações de revogação de certificados, incluindo publicação na sua página web.

4.9.11.2 Item não aplicável.

4.9.12 Requisitos especiais para o caso de comprometimento de chave
4.9.12.1. O titular de certificado deve notificar imediatamente, através de solicitação de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada

4.9.12.2. A perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de chave deve ser comunicado à AC DOCCLOUD RFB através do formulário específico para tal fim.

4.9.13 Circunstâncias para suspensão
Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de usuários finais.

4.9.14 Quem pode solicitar suspensão
A AC DOCCLOUD RFB, desde que aprovado pelo Comitê Gestor.

4.9.15 Procedimento para solicitação de suspensão
Os procedimentos de solicitação de suspensão serão dados por norma específica das DPC e PCs associadas.

4.9.16 Limites no período de suspensão
Os períodos de suspensão serão estabelecidos por norma específica das DPC e PCs associadas.

4.10 SERVIÇOS DE STATUS DO CERTIFICADO

4.10.1 Características operacionais
A AC DOCCLOUD RFB fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificado ou OCSP, 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 ENCARRAMENTO DE ATIVIDADES

4.11.1. A AC DOCCLOUD RFB observa os procedimentos descritos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.11.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC DOCCLOUD RFB segue os requisitos e procedimentos descritos no documento Plano de Encerramento. Esse plano tem abordagem multidisciplinar envolvendo aspectos de várias áreas da companhia, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC DOCCLOUD RFB:

a) Comunicará publicamente a extinção dos serviços da AC DOCCCLOUD RFB, através de publicação em jornal de grande circulação.
b) Revogará todos os certificados gerados pela AC DOCCLOUD RFB nos prazos estipulados nesta DPC, após a publicação e comunicará às partes afetadas através de mensagem eletrônica.
c) Extinguirá os serviços de emissão de certificados.

d) Extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços de status on-line após a revogação completa de todos os certificados.
e) Destruirá a chave privada da AC DOCCLOUD RFB extinta seguindo o procedimento descrito na DPC Item 6.2.9.
f) Transferirá os dados e gravações da AC DOCCLOUD RFB para a Autoridade Certificadora sucessora, aprovada pela AC Raiz. O período no qual eles ficarão armazenados está descrito na DPC item 4.6.
g) Transferirá as chaves públicas dos certificados emitidos pela AC DOCCLOUD RFB para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC DOCCLOUD RFB. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.
h) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC DOCCLOUD RFB.
i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

No caso de encerramento das atividades como AR vinculada a AC DOCCLOUD RFB a AR deverá seguir os seguintes requisitos e procedimentos:

a) Comunicará publicamente a extinção dos serviços de AR vinculada AC DOCCLOUD RFB, através de publicação em jornal de grande circulação.
b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados;
c) Ficará responsável pela guarda dos documentos, dados e registros relativos aos pedidos de emissão de certificados para a AC DOCCLOUD RFB, devendo fornecê-los sempre que solicitada pelo Titular, ou pela AC DOCCLOUD RFB. O período no qual eles ficarão armazenados está descrito na DPC item 4.6.

Em caso de falência ou extinção da AR a documentação e registros relativos à emissão de certificados deverá ser entregue para guarda da AC DOCCLOUD RFB.

No caso de encerramento das atividades como PSS vinculada a AC DOCCLOUD RFB, a AC DOCCLOUD RFB, diretamente ou por intermédio da AR, deverá seguir os seguintes requisitos e procedimentos:

a) Publicará, em sua página web, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso;
b) Manterá a guarda de toda a documentação comprobatória em seu poder.

4.12 CUSTÓDIA E RECUPERAÇÃO DA CHAVE

4.12.1 Política e práticas de custódia e recuperação de chave

Não é permitida a recuperação (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

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

A AC DOCCLOUD RFB não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1. Controles físicos

O acesso físico às dependências da AC DOCCLOUD RFB é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso. O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes. O sistema de certificação da AC DOCCLOUD RFB está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.1 Construção e localização das instalações de AC

5.1.1.1 A operação da AC DOCCLOUD RFB é executada dentro de um ambiente físico seguro em área de instalação altamente protegida. A localização e o sistema de certificação utilizado para a operação da AC DOCCLOUD RFB não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos. Nenhuma das linhas telefônicas dentro do ambiente de certificação da AC oferece suporte a modem.

5.1.1.2 Todas as instalações da AC DOCCLOUD RFB, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos a seguir:

a) todas as instalações de equipamentos de apoio, tais como: máquinas de ar-condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, retificadores, estabilizadores e similares;
b) instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas;
c) iluminação de emergência

5.1.2 Acesso físico

O acesso físico às dependências da AC DOCCLOUD RFB é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso. O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes. O sistema de certificação da AC DOCCLOUD RFB está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.2.1 Níveis de Acesso

5.1.2.1.1. São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC DOCCLOUD RFB, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

5.1.2.1.2. **O PRIMEIRO NÍVEL – OU NÍVEL 1** – Situa-se após a primeira barreira de acesso às instalações da AC DOCCLOUD RFB. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação da AC DOCCLOUD RFB transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC DOCCLOUD RFB é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido no ambiente onde estão instalados os equipamentos utilizados na operação da AC DOCCLOUD RFB, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, 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 nível. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas 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 DOCCLOUD RFB.

5.1.2.1.5. **O TERCEIRO NÍVEL – OU NÍVEL 3** – é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC DOCCLOUD RFB. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não estejam envolvidas com essas atividades não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

5.1.2.1.6. No terceiro nível 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: a identificação individual, como cartão eletrônico, e a identificação biométrica.

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

5.1.2.1.8. **O QUARTO NÍVEL - OU NÍVEL 4** – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da AC DOCCLOUD RFB, tais como: emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão 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 dessas pessoas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9. No quarto nível, todas as paredes, o piso e o teto são revestidos de aço e concreto ou de outro material 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. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem a chamada sala-cofre - possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. A sala-cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.

5.1.2.1.11. A AC DOCCLOUD RFB possui um único ambiente para abrigar os equipamentos de produção online, os equipamentos de produção off-line, o cofre de armazenamento e os equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

5.1.2.1.12. **O QUINTO NÍVEL – OU NÍVEL 5** – é interno aos ambientes de nível 4, e compreende cofres e gabinetes trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em nível 5 ou superior.

5.1.2.1.13. Para garantir a segurança do material armazenado o cofre ou o gabinete obedecem às seguintes especificações mínimas:

a) ser feito em aço ou material de resistência equivalente;

b) possuir tranca com chave.

5.1.2.1.14. **O SEXTO NÍVEL – OU NÍVEL 6** - consiste em pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da AC DOCCLOUD RFB estão armazenados em um desses depósitos

5.1.2.2. Sistema físico 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. As mídias de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da mídia) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma mídia referente a cada semana. Essas mídias são armazenadas em ambiente de terceiro 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. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.

5.1.2.2.4. Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar 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. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, é permanentemente monitorado por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

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 para garantir a segurança do pessoal e dos equipamentos da AC DOCCLOUD RFB em emergências. 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 estão documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de emergências.

5.1.3. Energia e Ar-condicionado
5.1.3.1. A infraestrutura do ambiente de certificação da AC DOCCLOUD RFB é 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 DOCCLOUD RFB e seus respectivos serviços. Um sistema de aterramento está implantado.

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

5.1.3.3. São utilizados tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São 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 aos 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 independente e tolerante a falhas.

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9. O sistema de ar condicionando dos ambientes de nível 4 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 é garantida por meio de:

a) geradores de porte compatível;
b) geradores de reserva;
c) sistemas de “no-breaks” redundantes;
d) sistemas redundantes de ar-condicionado.

5.1.4. Exposição à água
A estrutura inteiriça do 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. Todas as instalações da AC DOCCLOUD RFB possuem sistemas de prevenção contra incêndio. Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes 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 DOCCLOUD RFB não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. A sala cofre possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala cofre são eclusas, uma porta só se abre quando a anterior está fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC DOCCLOUD RFB, a temperatura interna da sala cofre não excede 50 graus Celsius e a sala suporta essa condição por, no mínimo, uma hora.

5.1.6. Armazenamento de mídia
A AC DOCCLOUD RFB atende a 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 documentados em papel que contenham 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)
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 tornar-se-ão totalmente operacionais em, no máximo, 48 (quarenta e oito) horas.

5.2. CONTROLES PROCEDIMENTAIS

5.2.1. Perfis qualificados
Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC DOCCLOUD RFB, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

5.2.1.1. A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2. A AC DOCCLOUD RFB estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as ações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

5.2.1.3. Todos os operadores do sistema de certificação da AC DOCCLOUD 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.

5.2.1.3.1 Item não aplicável.

5.2.1.4. Quando um empregado se desliga da AC, suas permissões de acesso são revogadas imediatamente.

Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC DOCCLOUD RFB, conforme o descrito em 6.2.2.

5.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC DOCCLOUD RFB necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC DOCCLOUD RFB. As demais tarefas da AC poderão ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1 Pessoas que ocupam os perfis designados pela AC DOCCLOUD RFB passam por um processo rigoroso de seleção. Todo funcionário da AC DOCCLOUD RFB tem sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso às instalações da AC DOCCLOUD RFB;
b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC DOCCLOUD RFB;
c) receber um certificado para executar suas atividades operacionais na AC DOCCLOUD RFB;
d) receber uma conta no sistema de certificação da AC DOCCLOUD RFB.

5.2.3.2. Os certificados, contas e senhas utilizadas para identificação e autenticação dos funcionários:

a) são diretamente atribuídos a um único operador (funcionário da AC DOCCLOUD RFB devidamente qualificado);
b) não são compartilhados;
c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC DOCCLOUD RFB implementa um padrão de utilização de "senhas fortes", definido em conformidade com a Política de Segurança da AC e DOCCLOUD 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 DOCCLOUD RFB impõe a separação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3. CONTROLES DE PESSOAL

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC DOCCLOUD RFB e pela AR DOCCLOUD 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 DOCCLOUD RFB e da AR DOCCLOUD, encarregados de tarefas operacionais, têm registrado em contrato ou termo de responsabilidade:

a) os termos e as condições do perfil que ocupam;
b) o compromisso de observar as normas, políticas e regras aplicáveis da AC DOCCLOUD RFB;
c) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
d) 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 DOCCLOUD RFB envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados são admitidos conforme o estabelecido na Política de Segurança da AC DOCCLOUD RFB e na Política de Segurança da ICP-Brasil [8].

5.3.2. Procedimentos de Verificação de Antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade da AC DOCCLOUD RFB, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, são submetidos aos seguintes processos, antes do começo das atividades de:

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 DOCCLOUD RFB poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC DOCCLOUD RFB e da AR vinculada, 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 DOCCLOUD RFB e da AR vinculada;
b) sistema de certificação em uso na AC DOCCLOUD RFB;
c) procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e da validade dos documentos apresentados, na forma dos itens 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 DOCCLOUD RFB e da Autoridade de Registro vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC DOCCLOUD RFB e no sistema das ARs.

5.3.5. Frequência e sequência de rodízios de cargos

A AC DOCCLOUD RFB não programa rodízio de cargos, de acordo com os propósitos estabelecidos no item 5.2.1 desta DPC para a definição de perfis qualificados.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC DOCCLOUD RFB suspenderá o seu acesso ao sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima conterá, no mínimo, os seguintes itens:

a) relato da ocorrência com “modus operandi”;
b) identificação dos envolvidos;
c) eventuais prejuízos causados;
d) punições aplicadas se for o caso; e
e) conclusões.

5.3.6.3. Concluído o processo administrativo, a AC DOCCLOUD RFB encaminhará suas conclusões à AC Raiz.

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

a) advertência;
b) suspensão por prazo determinado; ou
c) impedimento definitivo de exercer funções no âmbito da AC DOCCLOUD RFB e da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC DOCCLOUD RFB, das ARs Vinculadas, no exercício de atividades diretamente relacionadas com os

processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, será contratado conforme o estabelecido nas Política de Segurança da ICP-Brasil [8] e na Política de Segurança da AC DOCCLOUD RFB.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC DOCCLOUD RFB disponibiliza para todo o seu pessoal e para o pessoal das ARS vinculadas:

a) a DPC da AC DOCCLOUD RFB;
b) Item não aplicável;
c) a Política de Segurança da ICP-Brasil;
d) documentação operacional relativa às suas atividades;
e) contratos, normas e políticas relevantes para suas atividades; e
f) a Política de Segurança da AC DOCCLOUD RFB.

5.3.8.2. Toda a documentação é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC.

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

5.4.1. Tipos de Evento Registrados

5.4.1.1. A AC DOCCLOUD RFB registra em arquivos, para fins de auditoria, todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC DOCCLOUD RFB;
c) mudanças na configuração da AC DOCCLOUD 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 DOCCLOUD RFB ou de chaves de Titulares de Certificados;
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.

4.5.1.2. A AC DOCCLOUD RFB registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, quais sejam:

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. Os registros de auditoria mínimos a serem mantidos pela AC DOCCLOUD RFB incluem, além dos acima:

a) registros de solicitação, inclusive registros relativos a solicitações rejeitadas;
b) pedidos de geração de certificado, mesmo que a geração não tenha êxito;
c) registros de solicitação de emissão de LCR.

5.4.1.4. Todo o registro de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a

identidade do agente que o causou.

5.4.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC DOCCLOUD RFB é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil [8].

5.4.1.6. As AR vinculadas à AC DOCCLOUD RFB registram eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são 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; e
d) a assinatura digital do executante.

5.4.1.6.1 Item não aplicável.

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

5.4.2. Frequência de auditoria de registros (logs)

4.5.2.1. A análise dos registros de auditoria será realizada sempre que houver utilização de seu sistema de certificação (o equipamento é offline, permanecendo desligado a maior parte do tempo) ou em caso de suspeita de comprometimento da segurança.

4.5.2.2. Os registros de auditoria são analisados pela Área de Segurança da AC DOCCLOUD RFB. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando-se que não foram alterados, em seguida procede-se a 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 (logs) de Auditoria

A AC DOCCLOUD RFB mantém localmente, nas suas instalações, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 5.5.

5.4.4 Proteção de registros de auditoria

5.4.4.1. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção através das funcionalidades nativas dos sistemas operacionais. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, através de permissões dadas pelo administrador do sistema de acordo com a função dos usuários ou aplicações e orientação do departamento de segurança. O próprio sistema operacional também registra os acessos aos arquivos onde estão armazenados os registros de auditoria.

5.4.4.2. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção através de controles de acesso aos ambientes físicos onde são armazenados estes registros.

5.4.4.3. Os mecanismos de proteção descritos obedecem à Política de Segurança da AC DOCCLOUD RFB, em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.5 Procedimentos para cópia de segurança (Backup) de registros de auditoria

5.4.5.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC DOCCLOUD RFB, protegido com o mesmo tipo de proteção utilizada no arquivo principal.

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

5.4.6.3 A AC DOCCLOUD RFB garante que a verificação da integridade dessas cópias de segurança, é realizada no mínimo, a cada 6 (seis) meses.

5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)
O sistema de coleta de dados de auditoria da AC DOCCLOUD RFB é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC DOCCLOUD RFB, pelo sistema de controle de acesso e pelo pessoal operacional.

5.4.7 Notificação de agentes causadores de eventos
Eventos registrados pelo conjunto de sistemas de auditoria da AC DOCCLOUD RFB não são notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

5.4.8 Avaliações de vulnerabilidade
Uma Avaliação de Riscos de Segurança foi realizada para a AC DOCCLOUD RFB. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação. Eventos que indiquem possível vulnerabilidade, detectados na análise dos registros de auditoria da AC DOCCLOUD RFB, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

5.5. ARQUIVAMENTO DE REGISTROS

5.5.1. Tipos de registros arquivados
As seguintes informações são registradas e arquivadas pela AC DOCCLOUD RFB:

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 DOCCLOUD RFB;
g) informações de auditoria previstas no item 5.4.1;
h) correspondências formais;

5.5.2 Período de retenção para arquivo
Os períodos de retenção para cada registro arquivado são os seguintes:

a) as LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
b) as cópias dos documentos de identificação apresentados no momento da solicitação e da revogação de certificados e os termos de titularidade e responsabilidade serão retidos, no mínimo, por 7 (sete) anos a contar da data de expiração ou revogação do certificado; e
c) as demais informações, inclusive registros de auditoria são retidas por, no mínimo, 7 (sete) anos.

5.5.3 Proteção de arquivo
A AC DOCCLOUD RFB estabelece que todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis como tal classificação, conforme a Política de Segurança da AC DOCCLOUD RFB e POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.5.4 Procedimentos de cópia de arquivo
5.5.4.1. A AC DOCCLOUD RFB estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC DOCCLOUD RFB, 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 DOCCLOUD RFB verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5 Requisitos para datação de registros
5.5.5.1. Os servidores estão sincronizados com a Fonte Confiável de Tempo da AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário da Fonte Confiável de Tempo da AC

Raiz, inclusive os certificados emitidos por esses equipamentos.

5.5.5.2. No caso dos registros feitos manualmente e formulários de requisição de certificados, estes contêm a Hora Oficial do Brasil. Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

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 DOCCLOUD RFB em seus procedimentos operacionais são automatizados, manuais e internos.

5.5.7. Procedimentos para obter e verificar informação de arquivo
A verificação de informação de arquivo deve ser solicitada formalmente à AC DOCCLOUD RFB, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

5.6. TROCA DE CHAVE

5.6.1. O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico, disponibilizado pela AR Responsável, por onde é encaminhado o processo de fornecimento de novo certificado.

A AR que recebeu e validou o pedido de emissão do certificado envia uma comunicação ao titular do certificado 30 (trinta) dias antes da data de expiração do mesmo, juntamente com instruções para a solicitação de um novo certificado.

A comunicação de expiração, juntamente com as instruções para a solicitação de um novo certificado é realizada através de correio eletrônico enviado ao titular do certificado.

5.6.2. Item não aplicável.

5.7. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

Os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres estão descritos no Plano de Continuidade de Negócio – PCN da AC DOCCLOUD RFB, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento
5.7.1.1 A AC DOCCLOUD RFB deve possuir 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 previstos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs, contem 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, software ou dados corrompidos.
A AC DOCCLOUD RFB possui um PCN, de caráter sigiloso, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. O PCN especifica as ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

a) é feita a identificação de todos os elementos corrompidos;
b) o instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
c) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um *backup* de segurança até a revogação do certificado da AC DOCCLOUD RFB.

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 DOCCLOUD RFB a Diretoria, juntamente com a Supervisão de PKI da AC DOCCLOUD RFB, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC DOCCLOUD RFB emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

5.7.3.2 Chave de entidade é comprometida
Em caso de suspeita de comprometimento de chave da AC DOCCLOUD RFB, o fato é imediatamente comunicado a Diretoria que, juntamente com a Supervisão de PKI da AC DOCCLOUD RFB, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

a) Todos os certificados afetados serão revogados e as partes serão notificadas.
b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC DOCCLOUD RFB estiver encerrando suas atividades.

5.7.4 Capacidade de continuidade de negócio após desastre
Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de Infraestrutura, responsável pela contingência, notifica o Gerente de Segurança e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

a) garantir a integridade física das pessoas que se encontram nas instalações da AC DOCCLOUD RFB;
b) monitorar e controlar o foco da contingência;
c) minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

5.8. EXTINÇÃO DA AC DOCCLOUD RFB
CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICPBRASIL [6].

6. CONTROLES TÉCNICOS DE SEGURANÇA
Nos itens seguintes, a DPC define as medidas de segurança implantadas pela AC DOCCLOUD RFB para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. São também definidos outros controles técnicos de segurança utilizados pela AC DOCCLOUD RFB e pelas ARs vinculadas na execução de suas funções operacionais.

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1. Geração do Par de Chaves
6.1.1.1. O par de chaves criptográficas da AC DOCCLOUD RFB é gerado pela própria AC DOCCLOUD RFB, após ter sido credenciada e autorizada a funcionar no âmbito da ICP-Brasil.

A geração do par de chaves de AC DOCCLOUD RFB é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC DOCCLOUD RFB, treinados para a função.
A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves da AC DOCCLOUD RFB é gerado em módulos criptográficos de hardware, conforme definido no DOC-ICP-01.01, com padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5) definido no DOC-ICP-01.

6.1.1.2. A geração do par de chaves de AC DOCCLOUD RFB é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança, treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves da AC DOCCLOUD RFB é gerado em módulo criptográfico que adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

Os pares de chaves criptográficas são gerados somente pelo titular do certificado correspondente.

Os procedimentos específicos estão descritos em cada PC implementada pela AC DOCCLOUD RFB.

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

6.1.1.4. As chaves da AC DOCCLOUD RFB são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.1.5. Cada PC implementada pela AC DOCCLOUD RFB caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares dos 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 de geração de chaves assimétricas da AC DOCCLOUD RFB adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

Cada PC implementada específica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.1.2 Entrega da chave privada à entidade
A geração e a guarda de uma chave privada será de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3. Entrega da chave pública para emissor de certificado
6.1.3.1. Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC DOCCLOUD RFB fará uso do padrão PKCS#10, em data e hora previamente estabelecidas pela AC-Raiz da ICP-Brasil.

6.1.3.2. Os procedimentos para a entrega da chave pública de um solicitante de certificado estão detalhados nas PC implementadas.

6.1.4. Disponibilização de chave pública da AC DOCCLOUD RFB para usuários
As formas para a disponibilização do certificado da AC DOCCLOUD RFB e de todos os certificados da cadeia de certificação, para os usuários da AC DOCCLOUD RFB, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato definido

no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];
b) na página web: doccloud.com.br/repositorios/acdoccloudrfb
c) outros meios seguros aprovados pelo CG da ICP-Brasil

6.1.5. Tamanhos de chave

6.1.5.1. Cada PC implementada pela AC DOCCLOUD RFB define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento 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. Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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 [1].

6.1.7. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3)

6.1.7.1. As chaves criptográficas dos titulares de certificados emitidos pela AC DOCCLOUD RFB poderão ser utilizadas apenas para assinatura dos certificados por elas emitidos e de suas LCRs.

6.1.7.2. A chave privada da AC DOCCLOUD RFB é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCRs.

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

A AC DOCCLOUD RFB implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas.

A chave privada da AC DOCCLOUD RFB é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

Os titulares de certificados emitidos pela AC DOCCLOUD RFB, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado da suas chaves privadas

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC DOCCLOUD RFB adota o padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.2. Controle "n de m" para chave privada

6.2.2.1. A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC DOCCLOUD RFB é dividida em 8 (oito) partes e distribuídas por 8 (oito) custodiantes designados pela AC DOCCLOUD RFB (m).

6.2.2.2. É necessária a presença de no mínimo 2 (dois) custodiantes (n) para a ativação do componente e a consequente utilização da chave privada

6.2.3. Custódia (escrow) de chave privada

A AC DOCCLOUD RFB não implementa tal prática.

6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. Como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC DOCCLOUD RFB mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.

6.2.4.3. A AC DOCLCOUD RFB não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido. Por solicitação do respectivo titular ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC DOCCLOUD RFB poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo 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 ICPBRASIL [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. As chaves privadas dos titulares de certificados emitidos pela AC DOCCLOUD RFB não são arquivadas.

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

6.2.6. Inserção de chave privada em módulo criptográfico
A chave privada da AC DOCCLOUD RFB é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7 Armazenamento de chave privada em módulo criptográfico
Ver item 6.1.

6.2.8. Método de ativação de chave privada
A ativação das chaves privadas da AC DOCCLOUD RFB é implementada por meio do módulo criptográfico, após identificação dos operadores responsáveis. Esta identificação é realizada por meio de senha e de tokens ou cartões criptográficos, após a identificação de 2 (dois) dos 8 (oito) custodiantes da chave criptográfica de ativação. Os custodiantes da chave de ativação são funcionários indicados pelo representante legal da AC DOCCLOUD RFB.

6.2.9. Método de desativação de chave privada
A chave privada da AC DOCCLOUD RFB, armazenada em módulo criptográfico é desativada, quando não mais necessária, por meio de mecanismo disponibilizado pelo software de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de tokens ou cartões criptográficos, protegidos com senha, após a identificação de 2 (dois) dos 8 (oito) custodiantes da chave criptográfica de ativação.

6.2.10. Método de destruição de chave privada
Quando a chave privada da AC DOCCLOUD RFB for desativada, em decorrência de expiração ou revogação, ela deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, deve ser sobrescrito. Todas as cópias de segurança da chave privada da AC DOCCLOUD RFB e os cartões criptográficos dos custodiantes serão destruídos. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC DOCCLOUD RFB.

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. Arquivamento de chave pública
As chaves públicas da própria AC DOCCLOUD RFB, e dos titulares dos certificados por ela emitidos, bem como as LCR emitidas, serão armazenados pela AC DOCCLOUD RFB, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada
6.3.2.1. As chaves privadas dos titulares dos certificados de assinatura digital emitidos pela AC DOCCLOUD RFB são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo 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 DOCCLOUD RFB define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.4. A validade admitida para certificados de AC Subsequente é limitada à validade do certificado da AC DOCCLOUD RFB, desde que mantido o padrão de algoritmo para a geração de chaves assimétricas implementado

6.4. DADOS DE ATIVAÇÃO

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação da chave privada da AC DOCCLOUD RFB são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em hardware (token ou cartão criptográfico).

6.4.1.2. Item não aplicável.

6.4.2. Proteção dos dados de ativação.

6.4.2.1. Os dados de ativação das chaves privadas da AC DOCCLOUD RFB são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Item não aplicável.

6.4.3. Outros aspectos dos dados 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 AC DOCCLOUD RFB garante que a geração de seu par de chaves é realizada em ambiente offline, para impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC DOCCLOUD RFB são descritos em cada PC implementada.

6.5.1.3. Os computadores servidores, utilizados pela AC DOCCLOUD RFB, relacionados 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 DOCCLOUD RFB;
b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC DOCCLOUD RFB;
c) acesso restrito aos bancos de dados da AC DOCCLOUD RFB;
d) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
e) geração e armazenamento de registros de auditoria da AC DOCCLOUD RFB;
f) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
g) mecanismos para cópias de segurança (backup).

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

6.5.1.5. As informações sensíveis contidas nos equipamentos são retiradas dos equipamentos para manutenção. Os números de série dos equipamentos e as datas de envio e de recebimento da manutenção são controlados. Ao

retornar às instalações da AC DOCCLOUD RFB, o equipamento que passou por manutenção é inspecionado. As informações sensíveis armazenadas, relativas à atividade da AC DOCLCOUD RFB, são destruídas de maneira definitiva nos equipamentos que deixam de ser utilizados em carácter permanente. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC DOCCLOUD RFB é preparado e configurado como previsto na política de segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A AC DOCCLOUD RFB aplica configurações de segurança definidas como EAL3, baseadas no Common Criteria e desenvolvidas para o sistema operacional Red Hat Enterprise Linux. O fabricante disponibiliza as atualizações do sistema operacional utilizado nos servidores do Sistema de Certificação Digital da AC DOCCLOUD RFB.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1. Neste item estão descritos os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR para os processos de validação e aprovação de certificados.

6.5.3.2. Os requisitos abaixo correspondem aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

a) controle de acesso lógico ao sistema operacional;
b) exigência de uso de senhas fortes;
c) diretivas de senha e de bloqueio de conta;
d) 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 sistema dos operadores da AR;
    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
e) antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;
f) 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;
g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
h) sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
i) utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
j) impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
k) utilização de data e hora de Fonte Confiável do Tempo (FCT).

6.5.3.3. Item não aplicável.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1. A AC DOCCLOUD RFB adota sistema de certificação desenvolvido em código aberto; todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após a conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente de Operações da AC DOCCLOUD RFB avalia e decide quando será a implementação no ambiente de produção.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC DOCCLOUD RFB proverão documentação suficiente para suportar avaliações externas de segurança dos componentes da AC DOCCLOUD RFB.

6.6.2. Controle de gerenciamento de segurança

6.6.2.1. As ferramentas e os procedimentos empregados pela AC DOCCLOUD RFB para garantir que os seus sistemas implementem os níveis configurados de segurança são os seguintes:

a) a AC DOCCLOUD RFB opera em equipamento offline, portanto não necessita configuração de segurança de rede;

b) a administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional e pelos papéis confiados descritos no item 5.2.1.

6.6.2.2. O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC DOCCLOUD RFB, envolve testes de mudanças planejadas no Ambiente de Desenvolvimento e Homologação isolados antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

a) instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;

b) implantação ou modificação de Autoridades Certificadoras com customizações de certificados, páginas web, scripts etc.;

c) implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e

d) instalação de novos serviços na plataforma de processamento.

6.6.3. Controles de segurança de ciclo de vida

Item não aplicável.

6.6.4. Controles na Geração de LCR

Antes de publicadas todas as LCR geradas pela AC DOCCLOUD RFB são checadas quanto á consistência de seu conteúdo, comparando-a com o conteúdo esperado em relação ao 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. Neste item são descritos os controles relativos à segurança da rede da AC DOCCLOUD RFB, incluindo firewalls e recursos similares.

6.7.1.2. Nos servidores do sistema de certificação da AC DOCCLOUD 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 intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação 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 (GMUDs), 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 conectados a redes externas implementam filtros de pacotes de dados, que permitem somente as conexões aos serviços e servidores previamente 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. O firewall promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC DOCCLOUD RFB.

6.7.2.2. O software de firewall, entre outras características, implementa registros de auditoria.

6.7.3. Sistema de detecção de intrusão (IDS)

6.7.3.1. O sistema de detecção de intrusão está configurado para reconhecer ataques em tempo real e respondê-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 reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento.

6.7.3.3. O sistema de detecção de intrusão 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 – são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. CARIMBO DE TEMPO

Item não aplicável.

7. PERFIS DE CERTIFICADO E LCR

7.1. Perfil do Certificado

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

7.1.1. Número de versão

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

7.1.2. Extensões de 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 Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC DOCCLOUD RFB após conclusão do processo de seu credenciamento, é **2.16.76.1.1.71**.

7.1.7. Uso da extensão "Policy Constraints"
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.
Extensões críticas são interpretadas, no âmbito da AC DOCCLOUD RFB, conforme a RFC 5280
7.2. PERFIL DE LCR

7.2.1. Número (s) de versão
As LCR geradas pela AC DOCCLOUD 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. Neste item são descritas todas as extensões de LCR utilizadas pela AC DOCCLOUD RFB e sua criticalidade.

7.2.2.2. As LCR da AC DOCCLOUD RFB obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões para certificados de AC:

a) **"Authority Key Identifier"**, não crítica, contém o hash SHA-1 da chave pública da AC DOCCLOUD RFB que assina a LCR. As suítes de assinatura utilizadas na ICP-Brasil, baseiam-se no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];
b) **"CRL Number"**, não crítica: contém um número sequencial para cada LCR emitida pela AC DOCCLOUD RFB.

7.3. PERFIL DE OCSP

7.3.1. Número(s) de versão
Os serviços de respostas OCSP da AC DOCCLOUD RFB implementam a versão 1. do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP
Os serviços de respostas OCSP da AC DOCCLOUD RFB estão em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. FREQUÊNCIA E CIRCUNSTÂNCIA DAS AVALIAÇÕES

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

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

8.3. RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.3.1. Relação do avaliador com a entidade avaliada as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO

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

8.4.2. A AC DOCCLOUD 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 à AC DOCCLOUD RFB (AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC DOCCLOUD 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 DOCCLOUD RFB age de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.6. COMUNICAÇÃO DOS RESULTADOS

A AC DOCCLOUD RFB age de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. TARIFAS

9.1.1. Tarifas de emissão e renovação de certificados
Variável conforme definição interna comercial.

9.1.2. Tarifas de acesso ao certificado
Não são cobradas tarifas de acesso ao certificado digital emitido.

9.1.3. Tarifas de revogação ou de acesso à informação de status
Não são cobradas tarifas de revogação e de acesso à informação de status.

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

9.1.5. Política de reembolso

Em caso de revogação do certificado por motivo de comprometimento da chave privada ou da mídia armazenadora da chave privada da AC DOCCLOUD RFB, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC DOCCLOUD RFB, será emitido gratuitamente outro certificado em substituição.

9.2. RESPONSABILIDADE FINANCEIRA

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

9.2.1 Cobertura do 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

Conforme item 4 desta DPC.

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 ou às AR é sigiloso.

9.3.1.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AC DOCCLOUD RFB será divulgado.

9.3.2 Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas compreendem:

a) os certificados e a LCR emitidos pela AC DOCCLOUD RFB;
b) informações corporativas ou pessoais que façam parte do certificados ou em diretórios públicos;
c) esta DPC;
d) versões públicas da Política de Segurança;
e) resultados finais de auditorias; e
f) Termo de Titularidade ou solicitação de emissão do certificado.

A AC DOCCLOUD RFB e a AR a ela vinculada tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) estejam na posse legítima da AC DOCCLOUD RFB ou da AR a ela vinculada antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;
b) posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação sua sem quaisquer restrições para tal;
c) sejam requisitados por determinação judicial ou governamental, desde que a AC DOCCLOUD RFB ou a AR a ela vinculada comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC DOCCLOUD RFB e pela AR a ela vinculada, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

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.

9.3.2.1 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 DOCCLOUD RFB também são considerados documentos não confidenciais:

a) esta DPC;

b) versões públicas de Política de Segurança – PS; e
c) a conclusão dos relatórios da auditoria.

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

9.3.3.3. Os titulares de certificados emitidos para pessoas físicas ou 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 DOCCLOUD RFB assegurará a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2 Tratamento de informação como privadas
Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC DOCCLOUD RFB será 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/OCSP da AC DOCCLOUD RFB.

9.4.4 Responsabilidade para proteger a informação privadas
A AC DOCCLOUD RFB e AR são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 Aviso e consentimento para usar informações privadas
As informações privadas obtidas pela AC DOCCLOUD RFB poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável.

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.

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

As informações privadas ou confidenciais sob a guarda da AC DOCCLOUD 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
Como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC DOCCLOUD RFB deverá ser 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 DIREITOS DE PROPRIEDADE INTELECTUAL

De acordo com a legislação vigente

9.6 DECLARAÇÕES E GARANTIAS

9.6.1 Declarações e Garantias da AC DOCCOUD
A AC DOCCLOUD RFB declara e garante o quanto segue:

9.6.1.1 Autorização para certificado
A AC DOCCLOUD RFB implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC DOCCLOUD RFB, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das ARs vinculadas na forma de suas DPCs, PCs e normas complementares.

9.6.1.2 Precisão da informação
A AC DOCCLOUD RFB implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC.

A AC DOCCLOUD RFB, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das ARs vinculadas na forma de suas DPCs, PCs e normas complementares.

9.6.1.3 Identificação do requerente
A AC DOCCLOUD RFB implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC DOCCLOUD RFB, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ARs vinculadas na forma de suas DPCs, PCs e normas complementares.

9.6.1.4 Consentimento dos titulares
Consentimento dos titulares A AC DOCCLOUD RFB implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5 Serviço
A AC DOCCLOUD RFB mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios e LCRs.

9.6.1.6 Revogação
A AC irá revogar 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 DOCCLOUD
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 DOCCLOUD RFB, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2 A AC DOCCLOUD RFB deve informar 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 Um certificado emitido pela AC DOCCLOUD RFB é considerado válido quando:

i. tiver sido emitido pela AC DOCCLOUD RFB;
ii. não constar como revogado pela AC DOCCLOUD RFB;
iii. não estiver expirado; e
iv. puder ser verificado com o uso do certificado válido da AC DOCCLOUD RFB.

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 Representações e garantias de outros participantes

Item não aplicável

9.7 ISENÇÃO E GARANTIAS

Item não aplicável

9.8 LIMITAÇÕES DE RESPONSABILIDADE

A AC DOCCLOUD 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 DOCCLOUD 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 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. Procedimento para emendas
Qualquer alteração nesta DPC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos
A AC DOCCLOUD RFB mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web.

9.12.3. Circunstâncias 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 DOCCLOUD 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 DOCCLOUD 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 DOCCLOUD RFB e AR e outras entidades citadas. 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. Os documentos listados a seguir são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

REF	NOME DO DOCUMENTO	CÓDIGO
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001	DOC-ICP-02

10.2. Os documentos a seguir 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]	TERMO DE TITULARIDADE	ADE-ICP-05. B

11. REFERÊNCIAS BIBLIOGRÁFICAS

[5] WebTrust Principles and Criteria for Registration Authorities, disponível em http://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 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.