Declaração de Práticas de Certificação da Autoridade Certificadora da RFB

DPC AC - RFB

Secretaria da Receita Federal do Brasil

Versão 5.0 de 22/11/2012

Controle de Versão

Versão	Data	Motivo	Descrição
3.0	08/10/2002	Criação	Versão inicial
3.1	11/07/2008	Alteração	Adequações às Resoluções da ICP-Brasil
4.0	04/07/2011	Alteração	Atualizações de acordo com DOC-ICP-05 versão 3.5 e criação da AC-RFB v3 sob a cadeia da AC Raiz v2. Alterados os seguintes itens: 1.3.2.1, 1.4, 2.1.1, 2.1.3, 2.2.1.3, 2.6.1.2, 2.6.3, 3.1.1.5, 3.1.1.6, 3.2.2, 4.6.2, 5.1.2.1.11, 6.1.5, 6.7.1, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.2.8.2, 7.2.9, 7.3.1, 7.3.2, 8.1 e 9.3.
5.0	22/11/2012	Alteração	Resolução 90, de 13 de agosto de 2012, item 3.1.9.1

Sumário

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
ACT – Autoridade de Carimbo de Tempo
AR - Autoridades de Registro
CEI - Cadastro Específico do INSS
CG - Comitê Gestor
CMM-SEI - *Capability Maturity Model* do *Software Engineering Institute*
CMVP - *Cryptographic Module Validation Program*
CN - Common Name
CNE - Carteira Nacional de Estrangeiro
CNPJ - Cadastro Nacional de Pessoas Jurídicas -
COBIT - *Control Objectives for Information and related Technology*
COSO - *Comitee of Sponsoring Organizations*
CPF - Cadastro de Pessoas Físicas
DMZ - Zona Desmilitarizada
DN - *Distinguished Name*
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira
IDS - Sistemas de Detecção de Intrusão
IEC - *International Electrotechnical Commission*
ISO – *International Organization for Standardization*
ITSEC - *European Information Technology Security Evaluation Criteria*
ITU - *International Telecommunications Union*
LCR - Lista de Certificados Revogados
NBR - Norma Brasileira
NIS - Número de Identificação Social
NIST - *National Institute of Standards and Technology*
OCSP - *On-line Certificate Status Protocol*
OID - *Object Identifier*
OU - *Organization Unit*
PASEP - Programa de Formação do Patrimônio do Servidor Público
PC - Políticas de Certificado
PCN - Plano de Continuidade de Negócio
PIS - Programa de Integração Social
POP - *Proof of Possession*
PSS - Prestadores de Serviço de Suporte
RFC – *Request For Comments*
RG - Registro Geral
SINRIC – Sistema Nacional de Registro de Identificação Civil
SNMP - *Simple Network Management Protocol*
TCSEC - *Trusted System Evaluation Criteria*
TSDM - *Trusted Software Development Methodology*
UF - Unidade de Federação
URL - Uniform Resource Location

1. INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Este documento estabelece os requisitos mínimos a serem obrigatoriamente observados pela Autoridade Certificadora da Secretaria da Receita Federal do Brasil **(AC-RFB)**, integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. Esta DPC descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da RFB na execução dos seus serviços.

1.1.2 Esta DPC está em conformidade com o documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [1].

1.2 IDENTIFICAÇÃO

Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora da RFB”, integrante da ICP-Brasil, e comumente referida como “DPC AC-RFB”. O Object Identifier **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.8.**

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 Autoridades Certificadoras

Esta DPC refere-se, unicamente, à Autoridade Certificadora da Secretaria da Receita Federal do Brasil **(AC-RFB)** e encontra-se publicada na página http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf, bem assim na página http://www.receita.fazenda.gov.br/acrfb/dpcacrfb.pdf. A AC-RFB possui certificado de nível intermediário na ICP-Brasil assinado pela AC Raiz Brasileira.

1.3.2 Autoridades de Registro

1.3.2.1 A Autoridade de Registro da AC-RFB, doravante chamada de **AR-RFB**, é responsável pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais das Autoridades Certificadoras de nível imediatamente subseqüente ao da AC-RFB, e de identificação de seus solicitantes.

O endereço da página *web* (URL) da AC-RFB é http://www.receita.fazenda.gov.br/acrfb, onde estão publicados os dados de

identificação e endereçamento referentes à sua Autoridade de Registro, conforme itens “a” e “b” abaixo:

a) Identificação da AR credenciada (AR-RFB);
b) A instalação técnica da AR-RFB situa-se à SGAN 601 Módulo G, Bairro Asa Norte, Brasília / DF.

1.3.2.2 A AC-RFB mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A AC-RFB publica em sua página http://www.receita.fazenda.gov.br/acrfb identificação do seu Prestador de Serviço de Suporte.

1.3.3.2 PSS são entidades utilizadas pela AC-RFB ou pela AR-RFB para desempenhar as atividades descritas abaixo:

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

1.3.3.3 A AC-RFB mantém as informações acima sempre atualizadas.

1.3.4 Titulares de Certificado

A AC-RFB emite certificados para Autoridades Certificadoras de nível imediatamente subseqüente ao seu.

Os titulares dos certificados são as entidades pessoas jurídicas, autorizadas pela AR-RFB a receberem certificados digitais emitidos pela AC-RFB, credenciadas pela AC Raiz para integrar a ICP-Brasil e habilitadas pela RFB para emissão dos certificados definidos no documento “Leiaute de Certificados Digitais” da Secretaria da Receita Federal do Brasil.

Será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

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

1.3.5 Aplicabilidade

Os certificados definidos por esta DPC têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR), emitidos para as AC de nível imediatamente subseqüentes ao da AC-RFB.

1.4 DADOS DE CONTATO

Esta DPC é administrada pela Coordenação-Geral de Tecnologia da Informação (COTEC) da Secretaria da Receita Federal do Brasil, localizada no seguinte endereço:

Ministério da Fazenda, Anexo A, Sala 301.
Telefone: (550xx61) 3412-3708, 3412-3710, 3412-3713.
Fax: (550xx61) 3412-1533.
Página Web: http://www.receita.fazenda.gov.br.
E-mail: diseg.df@receita.fazenda.gov.br.

Pessoas de Contato.

Nome: Sérgio Roberto Fuchs da Silva.
Endereço: RFB – Ministério da Fazenda, Anexo A, Sala 315.
Telefone: (550xx61) 3412-3741.
Fax: (550xx61) 3412-1547.
E-mail: sergio.fuchs@receita.fazenda.gov.br.

2. DISPOSIÇÕES GERAIS

2.1 OBRIGAÇÕES E DIREITOS

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Caso haja obrigações específicas para as PC implementadas, as mesmas estarão descritas nessas PC, no item correspondente.

2.1.1 Obrigações da AC-RFB

As obrigações da AC-RFB são as abaixo relacionadas:

a) Operar de acordo com esta DPC;

b) Gerar e gerenciar o seu par de chaves criptográficas;

c) Assegurar a proteção de sua chave privada;

d) Notificar a AC Raiz da ICP-Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;

e) Notificar as AC de nível imediatamente subseqüente ao seu quando ocorrer: suspeita de comprometimento de sua chave, 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 das AC de nível imediatamente subseqüente ao seu;

h) Informar a emissão do certificado ao respectivo solicitante;

i) Revogar os certificados por ela emitidos;

j) Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);

k) Publicar em sua página *web:* http://www.receita.fazenda.gov.br/acrfb, a DPC AC-RFB aprovada e implementada;

l) Publicar em sua página *web* as informações definidas no item 2.6.1.2 desse documento;

m) Publicar, em página web, informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;

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 nesta DPC e na Política de Segurança que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios e procedimentos da ICP-Brasil;

q) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

r) Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

s) Manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;

t) Manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas AC de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;

u) Informar as terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC;

v) Informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos; e

w) Não emitir certificados com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações da AR-RFB

As obrigações da AR-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 à AC-RFB utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL[2];

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

e) Disponibilizar os certificados emitidos pela AC-RFB aos seus respectivos solicitantes;

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

g) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC-RFB e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL[2] ;

h) Manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP–Brasil;

i) Manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;

j) Proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10.

k) Garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas.

2.1.3 Obrigações do Titular do Certificado

As obrigações do titular de certificado emitido de acordo com esta DPC AC-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, senhas e dispositivos criptográficos;

c) Utilizar os seus certificados e suas respectivas chaves privadas de modo apropriado, conforme o previsto nesta DPC;

d) Conhecer os seus direitos e obrigações, contemplados pela DPC da AC-RFB, e por outros documentos aplicáveis da ICP-Brasil;

e) Informar à AC-RFB qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

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

2.1.4 Direitos da Terceira Parte (*Relying Party*)

2.1.4.1. Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

2.1.4.2. Constituem direitos da terceira parte:

a) Recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;
b) Verificar a qualquer tempo a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
   - Não constar da LCR da AC-RFB;
   - Não estiver expirado;
   - Puder ser verificado com o uso de certificado válido da AC-RFB.

2.1.4.3. O não exercício desses direitos não afasta a responsabilidade da AC-RFB e do titular do certificado.

2.1.5 Obrigações do Repositório

Em caso de uso do repositório, são obrigações do mesmo:

a) Disponibilizar, logo após a sua emissão, os certificados emitidos pela AC-RFB e a sua LCR;
b) Estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
c) Implementar os recursos necessários para a segurança dos dados nele armazenados.

2.2 RESPONSABILIDADES

2.2.1 Responsabilidades da AC-RFB

2.2.1.1. Não se aplica.

2.2.1.2. A AC-RFB responde solidariamente pelos atos das entidades de sua cadeia de certificação: AC subordinadas, AR e PSS.

2.2.1.3. Não se aplica

2.2.2 Responsabilidades da AR

A AR-RFB será responsável pelos danos a que der causa.

2.3 RESPONSABILIDADE FINANCEIRA

2.3.1 Indenizações devidas pela terceira parte (*Relying Party*)

Não existe responsabilidade da terceira parte (*Relying Party*) perante a AC-RFB ou a AR-RFB, que requeira prática de indenização, exceto na hipótese de prática de ato ilícito.

2.3.2 Relações Fiduciárias

A AC-RFB ou a AR-RFB indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3 Processos Administrativos

Será seguida legislação específica uma vez que a AC-RFB e a AR-RFB são administradas pela Secretaria da Receita Federal do Brasil - RFB, órgão da Administração Pública Federal.

2.4 INTERPRETAÇÃO E EXECUÇÃO

2.4.1 Legislação

Atos e regulamentos federais que regulam os assuntos do governo também regulam esta DPC no que diz respeito a sua aplicação, construção, interpretação e validade. Isto inclui leis e regulamentos que governam os seguintes relacionamentos:

a) Governo Federal e seus funcionários, incluindo empregados contratados por tempo indeterminado ou temporários e consultores sobre contrato;

b) Governo Federal e organizações do setor privado com relações de negócio estabelecidas;

c) Funcionários do Governo Federal com outros funcionários do Governo Federal.

A DPC AC-RFB obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil.

2.4.2 Forma de interpretação e notificação

2.4.2.1 Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, o corpo técnico da AC-RFB, examinará a disposição inválida e proporá nova redação ou retirada da disposição afetada. As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.2.2 Todas as solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa DPC serão realizadas, quando por iniciativa da AC-RFB, por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil e às AC subseqüentes se for o caso.

2.4.3 Procedimentos de solução de disputa

2.4.3.1 No caso de um conflito entre esta DPC e outras declarações, políticas, planos, acordos, contratos ou documentos que a AC-RFB adotar, esta DPC prevalecerá.

2.4.3.2 No caso de um conflito entre esta DPC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nesta situação esta DPC será alterada para a solução da disputa.

2.4.3.3 Os casos omissos serão encaminhados para a apreciação da AC Raiz.

2.5 TARIFAS DE SERVIÇO

Não há tarifas previstas pela AC-RFB para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.1 Tarifas de emissão e renovação de certificados

Não há tarifas previstas pela AC-RFB para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.2 Tarifas de acesso ao certificado

Não há tarifas previstas pela AC-RFB para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.3 Tarifas de revogação ou de acesso à informação de status

Não há tarifas previstas pela AC-RFB para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.4 Tarifas para outros serviços

Não há tarifas previstas pela AC-RFB para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.5 Política de reembolso

Não há política de reembolso prevista pela AC-RFB para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.6 PUBLICAÇÃO E REPOSITÓRIO

2.6.1 Publicação de informação da AC-RFB

2.6.1.1 A AC-RFB mantém página *web*, http://www.receita.fazenda.gov.br/acrfb, 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.

2.6.1.2 As seguintes informações são publicadas na página *web* da AC-RFB:

a) O certificado da AC-RFB;
b) Sua LCR;
c) Esta DPC;
d) Os certificados das AC de nível imediatamente subseqüente ao seu;
e) A AR vinculada (AR-RFB) e seu respectivo endereço de instalação técnica em funcionamento;
f) Legislação específica da RFB;
g) Documento "Leiaute de Certificados Digitais" da Secretaria da Receita Federal do Brasil.

2.6.2 Freqüência de publicação

Os certificados e a LCR são publicados imediatamente após sua emissão pela AC-RFB. As demais informações mencionadas no item 2.6.1 serão publicadas sempre que sofrerem alterações.

2.6.3 Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, aos certificados emitidos e à LCR da AC-RFB.

Acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controle de acesso incluirão identificação pessoal para acesso aos equipamentos e utilização de senhas.

2.6.4 Repositórios

A AC-RFB utiliza sua página *web* como repositório das informações que publica, e atende aos seguintes requisitos:

a) Localização: http://www.receita.fazenda.gov.br/acrfb;
b) Disponibilidade: aquela definida no item 2.6.1.1 desta DPC;
c) Protocolos de acesso: HTTP e HTTPS;
d) Requisitos de segurança: obedece aos requisitos definidos no item 5 desta DPC AC-RFB.

2.7 FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE

2.7.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades da AC-RFB e da AR-RFB estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.2. As fiscalizações da AC-RFB e da AR-RFB são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

2.7.3. A auditoria da AC-RFB e da AR-RFB é realizada pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [4].

2.7.4. A AC-RFB informa que recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e que 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 [4].

2.7.5. AR-RFB também recebeu auditoria prévia, para fins de credenciamento.

2.8 SIGILO

2.8.1 Disposições Gerais

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

2.8.1.2 Os titulares de certificados emitidos pela AC-RFB, ou os responsáveis pelo seu uso, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, são responsáveis pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1.3 A AC-RFB não emite certificados de sigilo.

2.8.2 Tipos de informações sigilosas

2.8.2.1 Todas as informações coletadas, geradas, transmitidas e mantidas pela AC-RFB e pela AR-RFB são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3.

2.8.2.2 Como princípio geral, nenhum documento, informação ou registro fornecido à AC-RFB ou AR-RFB deverá ser divulgado.

2.8.3 Tipos de informações não sigilosas

Os seguintes documentos e informações da AC-RFB e AR-RFB são considerados não sigilosos:

a) Os certificados e as LCR emitidos;
b) Informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
c) A PC implementada pela AC;
d) A DPC da AC;
e) Versões públicas de Políticas de Segurança;
f) A conclusão dos relatórios de auditoria.

2.8.4 Divulgação de informação de revogação ou suspensão de certificado

2.8.4.1. A AC-RFB divulga informações de revogação dos certificados por ela emitidos, na sua página *web* descrita no item 2.6.1 desta DPC, através de sua lista de certificados revogados.

2.8.4.2. As razões para revogação do certificado sempre serão informadas para o seu titular.

2.8.4.3. A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

2.8.5 Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertença ou esteja sob a guarda da AC-RFB e sua AR-RFB é divulgado a entidades legais ou seus funcionários, exceto quando:

- Exista uma ordem judicial corretamente constituída;
- Esteja corretamente identificado o representante da lei.

2.8.6 Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro, sob a guarda da AC-RFB ou AR-RFB, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

2.8.7 Divulgação por solicitação do titular

2.8.7.1. 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.

2.8.7.2. Qualquer liberação de informação pela AC-RFB ou AR-RFB, somente será permitida mediante autorização formal do titular do certificado. As formas de autorização são as seguintes:

- Por meio eletrônico, contendo assinatura válida garantida por certificado do titular, reconhecida pela AC-RFB; ou
- Por meio de pedido escrito com firma reconhecida.

2.8.8 Outras circunstâncias de divulgação de informação

Nenhuma outra liberação de informação, que não as expressamente descritas nesta DPC, é permitida.

2.9 DIREITOS DE PROPRIEDADE INTELECTUAL

Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, e todos os documentos gerados para a AC-RFB (eletrônicos ou não), de acordo com a legislação vigente, pertencem e continuarão sendo propriedade da Secretaria da Receita Federal do Brasil – RFB.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 REGISTRO INICIAL

3.1.1 Disposições Gerais

3.1.1.1. Neste item e nos seguintes esta DPC descreve os requisitos e os procedimentos gerais utilizados pela AR-RFB, vinculada à AC-RFB, responsável para a realização dos seguintes processos:

a) Validação da solicitação de certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado com base nos documentos de identificação citados nos itens 3.1.9 (autenticação da identidade de um individuo) e 3.1.10 (Autenticação da identidade de uma organização) desta DPC, realizada simultaneamente por pelo menos dois agentes de registro.

i. Confirmação da identidade de um indivíduo: comprovação de que a pessoa física que se apresenta como titular pelo certificado da AC subseqüente a AC-RFB e como representante legal da pessoa jurídica, credenciada pelo ITI e

habilitada pela RFB, é realmente aquela cujos dados constam na documentação apresentada;

ii. Confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado de AC subseqüente a AC-RFB e de que a pessoa física que se apresenta como representante legal da pessoa jurídica, credenciada pela ITI e habilitada pela RFB, realmente possui tal atribuição;

iii. Emissão do certificado: conferência dos dados do Formulário de Solicitação de Emissão de Certificado Para Desenvolver Atividades de Autoridade Certificadora Habilitada com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC-RFB.

b) Verificação da solicitação de certificado - não se aplica, uma vez que a AC *offline* pressupõe que o trabalho seja realizado uma única vez, simultaneamente pelos Agentes de Registro, em conformidade com o item anterior.

3.1.1.2. Os itens i e ii do processo de validação são realizados pelos agentes de registro fora do ambiente físico da AR-RFB.

3.1.1.3. A etapa iii do processo de validação de certificado são registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC-RFB, com a utilização de certificado digital no mínimo do tipo A3. Tais registros serão feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4. É mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias serão mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [2].

3.1.1.5. Não se aplica.

3.1.1.6. Não se aplica.

3.1.2 Tipos de nomes

3.1.2.1. As AC de nível imediatamente subseqüente ao da AC-RFB, titulares de certificados de AC habilitada, terão um nome que as identifique univocamente no âmbito da AC-RFB, no padrão ITU X.500.

3.1.2.2. A AC-RFB não inclui no certificado das AC subseqüentes o nome da pessoa física responsável pelo mesmo.

3.1.3 Necessidade de nomes significativos

Para identificação dos titulares dos certificados emitidos, a AC-RFB faz uso de nomes significativos que possibilitam determinar a identidade da organização a que se referem.

3.1.4 Regras para interpretação de vários tipos de nomes

Item não aplicável.

3.1.5 Unicidade de nomes

Os identificadores "*Distinguished Name"* (DN) são únicos para cada AC de nível imediatamente subseqüente ao da AC-RFB. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509.

3.1.6 Procedimento para resolver disputa de nomes

A AC-RFB reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes das AC de nível imediatamente subseqüente ao seu. Durante o processo de confirmação de identidade, a AC solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.8 Método para comprovar a posse de chave privada

A confirmação que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, item 2.3, relativos ao *"Proof of Possession (POP) of Private Key".*

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade da pessoa física responsável pela AC de nível imediatamente subseqüente ao da AC-RFB é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

3.1.9.1. Documentos para efeito de identificação de um indivíduo

As solicitações de certificados, para as AC subordinadas, devem ser realizadas por pessoa física legalmente responsável, que deverá apresentar a seguinte documentação, em sua versão original acompanhada de cópia legível e que permita a identificação do solicitante:

a) Cédula de identidade ou passaporte se brasileiro;
b) Cadastro de Pessoa Física;
c) Carteira nacional de estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
d) Passaporte se estrangeiro, não domiciliado no Brasil;
e) Caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos, ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data de validação presencial;

f) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data de validação presencial.

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

NOTA 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

NOTA 4: Não se aplica.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento preferencialmente a CNH – Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

NOTA 6: Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERISTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

NOTA 7: Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

NOTA 8: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

NOTA 9: O cartão CPF poderá ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.9.2.1. Não se aplica.

3.1.9.2.2. Não se aplica.

3.1.9.2.3. Não se aplica.

3.1.10 Autenticação da Identidade de uma organização

3.1.10.1. **Disposições Gerais**

3.1.10.1.1. Os procedimentos empregados pela AR-RFB para a confirmação da identidade de uma AC subordinada são feitos mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

3.1.10.1.2. Os titulares dos certificados são pessoas jurídicas, autorizadas pela AR-RFB a receberem certificados digitais emitidos pela AC-RFB, credenciadas pela AC Raiz para integrar a ICP-Brasil e habilitadas pela RFB para emissão de certificados definidos no documento “Leiaute de Certificados Digitais” da RFB. Será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

3.1.10.1.3. A confirmação da identidade da pessoa jurídica responsável pela solicitação de certificado de AC de nível imediatamente subseqüente ao da AC-RFB e da pessoa física representante legal pela referida AC será feita nos seguintes termos:

a) Apresentação do rol de documentos elencados no item 3.1.10.2 - Pessoa Jurídica;
b) Apresentação do rol de documentos elencados no item 3.1.9.1 do(s) - representante(s) legal(is) da pessoa jurídica;
c) Presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade de que trata o item 4.1.1.

3.1.10.2. **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 a sua habilitação jurídica:

i. se pessoa jurídica criada ou autorizada a sua criação por lei:
- Ato constitutivo, devidamente registrado no órgão competente; e
- Documento de nomeação do responsável emitido pela autoridade competente.

ii. se entidade privadas
- ato constitutivo, devidamente registrado no órgão competente; e
- Documento da eleição de seus administradores, quando aplicável.

b) Relativos a 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.

3.1.10.3. **Informações contidas no certificado emitido para uma organização**

Não se aplica.

3.1.11 Autenticação da Identidade de um equipamento ou aplicação

Não se aplica.

3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

3.2.1. O processo de identificação do solicitante quando da geração de novo par de chaves e emissão pela AC-RFB de novo certificado, antes da expiração do atual, será realizado em conformidade com o item 3.1.9 e 3.1.10.

3.2.2. Esse processo será conduzido da seguinte forma:

a) Adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;
b) Não se aplica;
c) Em caso de pessoa jurídica, qualquer alteração em sua constituição e funcionamento deverá constar do processo de renovação.

3.2.3. Não se aplica.

3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO

3.3.1. O processo de identificação do solicitante quando da geração de novo par de chaves e emissão pela AC-RFB de novo certificado, após expiração ou revogação do anterior, será realizado em conformidade com o item 3.1.9 e 3.1.10.

3.3.2. Após a expiração ou revogação de seu certificado a AC de nível imediatamente subseqüente ao da AC-RFB deve executar os processos regulares de geração de novo par de chaves. Serão adotados os mesmos requisitos e procedimentos exigidos inicialmente para a emissão do novo certificado.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

Somente os agentes descritos no item 4.4.2 podem solicitar a revogação do certificado de uma AC de nível imediatamente subseqüente ao da AC-RFB.

Quando realizada por solicitação da AC titular do certificado, em conformidade com a alínea “a” do item 4.4.2 desta DPC, a solicitação de revogação de certificado da AC imediatamente subseqüente será feita formalmente pelo representante legal da respectiva AC, e com a presença física do mesmo, a fim de possibilitar a sua identificação inequívoca. O processo de identificação do solicitante será conforme o item 3.1.9 e 3.1.10.

O procedimento para solicitação de revogação de certificado pela AC-RFB está descrito no item 4.4.3.

As solicitações de revogação de certificados são obrigatoriamente documentadas.

4. REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

4.1.1. Os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado são:

a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.1;

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

c) Assinatura do Termo de Titularidade.

4.1.2. A solicitação de certificado para AC de nível imediatamente subseqüente ao da AC-RFB somente é possível após o deferimento do pedido de credenciamento e a respectiva autorização de funcionamento da AC em questão pela AC-Raiz, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.3. Nesse caso, a AC subseqüente deve encaminhar a solicitação de seu certificado à AC-RFB por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

4.2 EMISSÃO DE CERTIFICADO

4.2.1. A emissão de um certificado pela AC-RFB é feita em cerimônia específica, com a presença dos representantes da AC-RFB, da AC habilitada e convidados, na qual são registrados todos os procedimentos executados.

a) AC-RFB garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subseqüente ao seu ocorre em, no máximo, 10 (dez) dias úteis após a autorização de funcionamento da AC em questão pela AC-RAIZ.

b) A AC-RFB entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC habilitada.

c) A emissão dos certificados das AC de nível imediatamente subseqüente à AC-RFB é feita em equipamentos que operam *offline*.

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

4.3 ACEITAÇÃO DE CERTIFICADO

4.3.1. O processo de aceitação de um certificado emitido pela AC-RFB a uma AC subseqüente se dará em duas etapas: na cerimônia de emissão do certificado,

perante os representantes legais da mesma, e após sua utilização no ambiente operacional da AC subseqüente.

4.3.2. A AC de nível imediatamente subseqüente irá declarar, através de seus representantes legais, mediante assinatura do "Termo de Acordo", que aceita o certificado emitido. A aceitação implica que o solicitante reconhece a veracidade dos dados contidos no certificado.

4.3.3. A AC-RFB mantém o documento "Termo de Acordo" onde o representante legal da AC subseqüente declara a aceitação do certificado.

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 Circunstâncias para revogação

4.4.1.1. Um certificado de AC de nível imediatamente subseqüente ao da AC-RFB pode ser revogado a qualquer momento por solicitação da AC titular do certificado, por decisão da AC-RFB , do CG da ICP-Brasil ou da AC Raiz.

4.4.1.2. Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

a) Quando constatada emissão imprópria ou defeituosa;
b) Quando for necessária a alteração de qualquer informação constante no mesmo;
c) No caso de dissolução da AC titular do certificado;
d) No caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.4.1.3. Em relação à revogação, deve ainda ser observado que:

a) A AC-RFB revogará, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil;
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 pela ICP-Brasil.

4.4.2 Quem pode solicitar revogação

A revogação do certificado de uma AC de nível imediatamente subseqüente ao da AC-RFB somente pode ser feita:

a) Por solicitação da AC Titular do Certificado;
b) Por determinação da AC-RFB;
c) Por solicitação da AR-RFB;
d) Por determinação do CG da ICP-Brasil;
e) Por determinação da AC Raiz;

4.4.3 Procedimento para solicitação de revogação

4.4.3.1. A solicitação de revogação de certificado de AC de nível imediatamente subseqüente ao da AC-RFB é efetivada através do Formulário de Solicitação de Revogação de Certificado de Autoridade Certificadora Habilitada, preenchido pelo representante legal da AC e assinado no ato de entrega, realizada pessoalmente à AC-RFB.

4.4.3.2. 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 serão registradas e armazenadas;
c) As justificativas para a revogação de um certificado serão documentadas;
d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.4.3.3. Não se aplica.

4.4.3.4. O prazo limite para a conclusão do processo de revogação de certificado de AC subseqüente, após o recebimento da respectiva solicitação é de 12 (doze) horas.

4.4.3.5. A AC-RFB responde plenamente por todos os danos causados pelo uso do certificado da AC subseqüente, no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.4.3.6. Não se aplica.

4.4.4 Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1.

4.4.4.2. Não se aplica.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-RFB.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-RFB.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-RFB.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-RFB.

4.4.9 Freqüência de emissão de LCR

4.4.9.1. O prazo máximo admitido para a emissão de LCR referente a certificados de AC subordinadas é de 45 (quarenta e cinco) dias.

4.4.9.2. Não se aplica.

4.4.9.3. Em caso de revogação de certificado de AC de nível imediatamente subseqüente ao seu, a AC-RFB emitirá nova LCR no prazo previsto no item 4.4.3 e notificará todas as AC de nível imediatamente subseqüentes.

4.4.9.4. Não se aplica.

4.4.10 Requisitos para verificação de LCR

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

4.4.10.2. A autenticidade da LCR deve também ser confirmada por meio da verificação da assinatura da AC-RFB e do período de validade da LCR.

4.4.10.3. Os números de série de certificados de qualquer entidade final que estejam revogados aparecem na LCR emitida pela AC-RFB. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após data de suas expirações.

4.4.11 Disponibilidade para revogação/verificação de status *online*

A AC-RFB não disponibiliza recursos para revogação ou verificação *online* de status de certificados.

4.4.12 Requisitos para verificação de revogação *online*

A AC-RFB não disponibiliza diretório *online* ou um servidor de OCSP para verificar o estado dos certificados emitidos pela AC-RFB.

4.4.13 Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subseqüente ao da AC-RFB serão divulgadas por meio da página *web (*http://www.receita.fazenda.gov.br/acrfb da RFB.

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

Item não aplicável.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. No caso do comprometimento da chave privada de uma AC de nível imediatamente subseqüente ao da AC-RFB, a mesma deve notificar imediatamente à AC-RFB, solicitando a revogação de seu certificado, conforme descrito no item 4.4.3 desta DPC.

4.4.15.2. O meio utilizado para comunicação do comprometimento ou a suspeita de comprometimento de chave será por intermédio de correspondência assinada utilizando, ainda, procedimento que resguarde o sigilo da informação.

4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1 Tipos de Evento Registrados

4.5.1.1. Todas as ações executadas pelo pessoal da AC-RFB, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A AC-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-RFB;
c) Mudanças na configuração da AC-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-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;
l) Operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A AC-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) Registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

4.5.1.3. Os registros de auditoria mínimos a serem mantidos pela AC-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.

4.5.1.4. Todos os registros de auditoria, eletrônicos ou manuais, contêm a data e a hora do evento registrado e a identidade do agente que o causou.

4.5.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC-RFB é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.1.6. Não se aplica.

4.5.1.7. A AC-RFB define como local de arquivamento dos documentos, utilizados para identificação do Titular do Certificado e da pessoa jurídica a Divisão de Segurança da Informação – DISIN/COTEC/RFB.

4.5.2 Freqüência de auditoria de registros (*logs*)

A auditoria de registro será realizada sempre que houver utilização do sistema de certificação.

Os registros de auditoria são analisados pelo pessoal operacional da AC-RFB em período não superior a uma semana. 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.

4.5.3 Período de Retenção para registros (*logs*) de Auditoria

A AC-RFB mantém localmente, nas instalações do Centro de Certificação Digital do SERPRO/RJ (CCD), os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4 Proteção de registro (*log*) de Auditoria

4.5.4.1. Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.4.2. As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.4.3. Os mecanismos de proteção descritos neste item obedecem a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.5 Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria

A AC-RFB executa procedimentos de backup de todo o sistema de certificação, em período não superior a uma semana ou sempre que houver utilização do mesmo, seguindo scripts previamente desenvolvidos para estas atividades.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é interno à AC-RFB e utiliza processos manuais e automatizados.

4.5.7 Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC-RFB não são notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8 Avaliações de vulnerabilidade

Eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC-RFB, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

4.6 ARQUIVAMENTO DE REGISTROS

4.6.1 Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC-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-RFB;
g) Informações de auditoria previstas no item 4.5.1.

4.6.2 Período de retenção para arquivo

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

a) As LCR referentes a certificados de assinatura digital são retidas permanentemente para fins de consulta histórica;
b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. **As prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado;** e
c) As demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 6 (seis) anos.

4.6.3 Proteção de arquivos

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.6.4 Procedimentos para cópia de segurança (*backup*) de arquivos

4.6.4.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC-RFB, e recebem o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

4.6.4.3. É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.6.5 Requisitos para datação de registros

Os servidores da AC-RFB são sincronizados com a hora GMT fornecida pelo Observatório Nacional. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.
No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.6 Sistema de coleta de dados de arquivo

O sistema de coleta de dados de arquivos da AC-RFB é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
Solicitações de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados	Automático	*Software* de AC/AR
Emissões de LCR	Automático	*Software* de AC/AR

4.6.7 Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC-RFB e da AR-RFB é verificada:

a) Na ocasião em que o arquivo é preparado;
b) Semestralmente no momento de uma auditoria de segurança programada;
c) Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

4.7 TROCA DE CHAVE

4.7.1. A AC-RFB comunica através de oficio, com 90 dias de antecedência, à AC subseqüente o vencimento do seu certificado, junto com as informações necessárias para a solicitação de uma nova chave.

4.7.2. Não se aplica.

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

Nos itens seguintes estão descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no PCN da AC-RFB, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

4.8.1 Recursos computacionais, *software* e dados corrompidos

A AC-RFB possui um Plano de Continuidade de Negócio que 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-RFB.

4.8.2 Certificado de entidade é revogado

A AC-RFB possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que o certificado da AC-RFB é revogado, e que podem ser resumidas da seguinte forma:

- Em caso de revogação do certificado da AC-RFB, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados das AC de nível imediatamente subseqüente. É gerado, então, o novo par de chaves da AC-RFB e emitido pela AC Raiz certificado associado ao novo par de chaves gerado e emitidos, pela AC-RFB, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.3 Chave de entidade é comprometida

A AC-RFB possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que a chave privada da AC-RFB é comprometida, e que podem ser resumidas nas ações listadas a seguir:

- Em caso de comprometimento da chave da AC-RFB, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC-RFB e das AC de nível imediatamente subseqüente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-RFB, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

A AC-RFB possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC-RFB quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC-RFB faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a AC-RFB para tornar acessível os

registros lógicos mantidos dentro do *software*. Serão tomadas as ações de recuperação aprovadas dentro do plano segundo uma ordem de prioridade.

4.8.5 Atividades das Autoridades de Registro

Os procedimentos previstos no PCN da AR-RFB vinculada para recuperação, total ou parcial de suas atividades, contem, no mínimo as seguintes informações:

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo, falha de equipamentos, inundações e incêndios;
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. Atenção especial deve ser dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;
d) documentação dos processos e procedimentos acordados;
e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
f) teste e atualização dos planos.

4.9 EXTINÇÃO DOS SERVIÇOS DA AC, AR OU PSS

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

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

a) Prover com maior antecedência possível notificação para:
    1. A AC Raiz da ICP-Brasil;
    2. Todas as entidades subordinadas.
b) A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-RFB ou para a AR-RFB extinta;
c) Preservar qualquer registro não transferido a um sucessor;
d) As chaves públicas dos certificados emitidos pela AC-RFB, dissolvida, serão armazenadas por outra AC, após aprovação da AC Raiz;
e) Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC-RFB;
f) A AC-RFB, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas;
g) Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes estão descritos os controles de segurança implementados pela AC-RFB e pela AR-RFB para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 CONTROLE FÍSICO

5.1.1 Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação utilizado para a operação da AC-RFB não são publicamente identificados. Não há identificação pública externa das instalações e, 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.

5.1.1.2. Todos os aspectos de construção das instalações da AC-RFB, relevantes para os controles de segurança física, foram executados por técnicos especializados, especialmente os descritos abaixo:

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 e estabilizadores e similares;
b) Instalações para sistemas de telecomunicações;
c) Sistema de aterramento e de proteção contra descargas atmosféricas;
d) Iluminação de emergência.

5.1.2 Acesso físico nas instalações de AC

O acesso físico às dependências da AC-RFB é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

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-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-RFB. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC-RFB transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC-RFB é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC-RFB, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem 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 e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC-RFB. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico, e o uso de crachá.

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-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 possuem permissão de acesso 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-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-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. 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 deverão ser sanadas por normas internacionais pertinentes.

5.1.2.1.11. São três os tipos de serviço abrigados no ambiente de quarto nível:
a) Equipamentos de produção *online* e cofre de armazenamento;
b) Equipamentos de produção *offline* e cofre de armazenamento;
c) 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 reforçados trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre e 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 de 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-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 câmaras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 1 (um) ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas 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.

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, são permanentemente monitorados 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-RFB em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

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

5.1.3 Energia e ar condicionado nas instalações da AC

5.1.3.1. A infraestrutura do ambiente de certificação da AC-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-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 utilizadas 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 à 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 nas instalações da AC

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 nas instalações da AC

5.1.5.1. 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 sobre-aquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2. Nas instalações da AC-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 esta fechada.

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

5.1.6 Armazenamento de mídia nas instalações da AC

A AC-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 nas instalações da AC

5.1.7.1. Todos os documentos 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 (*offsite*) para AC

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

5.1.9 Instalações técnicas de AR

As instalações técnicas de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL [2].

5.2 CONTROLES PROCEDIMENTAIS

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC-RFB e na AR-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 Perfis qualificados

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 o seu perfil.

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

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

5.2.1.4. Quando um empregado se desliga da AC-RFB, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC-RFB, 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-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-RFB necessitam da presença de no mínimo 2 (dois) operadores (funcionários com perfis qualificados) da AC-RFB. As demais tarefas da AC-RFB podem ser executadas por um único operador.

5.2.3 Identificação e autenticação para cada perfil

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

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

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

a) São diretamente atribuídos a um único operador (funcionário da AC-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-RFB implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas.

5.3 CONTROLES DE PESSOAL

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC-RFB, pelas AR e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. A DPC garante que todos os empregados da AC-RFB e das

AR e PSS vinculados, 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-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-RFB e AR-RFB envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC-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-RFB, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é submetido 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-RFB poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal da AC-RFB e da AR-RFB, 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 temas, relacionados ao perfeito desempenho de suas atividades. Os temas deverão abordar, dentre outros e quando cabíveis, os seguintes assuntos:

a) Princípios e mecanismos de segurança da AC-RFB e da AR-RFB;
b) Sistema de certificação em uso na AC-RFB;
c) Procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9 e 3.1.10;
e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Freqüência e requisitos para reciclagem técnica

Todo o pessoal da AC-RFB e da AR-RFB 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-RFB ou da AR-RFB. Treinamentos de reciclagem são realizados pela AC-RFB sempre que necessário.

5.3.5 Freqüência e seqüência de rodízios de cargos

A AC-RFB não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC-RFB ou da AR-RFB, é suspenso, de imediato, o acesso dessa pessoa ao seu sistema de certificação, é instaurado processo administrativo para apurar os fatos e, se for o caso, adotadas as medidas 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) conclusões.

5.3.6.3. Concluído o processo administrativo, a AC-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;
c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 Requisitos para contratação de pessoal

O pessoal da AC-RFB e da AR-RFB, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é contratado conforme o estabelecido na Política de Segurança da AC-RFB e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.3.8 Documentação fornecida ao pessoal

5.3.8.1.A AC-RFB disponibiliza para todo o seu pessoal e para a AR-RFB:

a) Esta DPC;

b) A PC que implementa;
c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8];
d) A Política de Segurança da AC-RFB;
e) Documentação operacional relativa às suas atividades;
f) Contratos, normas e políticas relevantes para suas atividades.

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

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes estão definidas as medidas de segurança implantadas pela AC-RFB para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. Estão também definidos outros controles técnicos de segurança utilizados pela AC e pela AR-RFB 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 da AC-RFB é gerado pela própria AC-RFB, em módulo criptográfico de *hardware* com padrão de segurança definido pelo DOC-ICP-01.01, item 3, utilizando algoritmo RSA para geração do par de chaves e algoritmo 3-DES para sua proteção, após o deferimento do pedido de credenciamento da mesma e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. O par de chaves criptográficas de uma AC de nível imediatamente subseqüente ao da AC-RFB é gerado pela própria AC, após o deferimento do pedido de credenciamento e habilitação da mesma, e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil. Ao ser gerada, a chave privada da entidade titular é gravada cifrada por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em *hardware* criptográfico com padrão de segurança definido pelo DOC-ICP-01.01, item 3. A chave privada trafega cifrada, empregando os mesmos algoritmos citados anteriormente, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento. O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada é única e seu sigilo é suficientemente assegurado;
b) A chave privada não pode, com uma segurança razoável, ser deduzida;
c) A chave privada está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
d) A chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.3. Não se aplica.

6.1.2 Entrega da chave privada à entidade titular

É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

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-RFB fará uso do padrão PKCS#10, em data e hora previamente estabelecidos pela AC-Raiz da ICP-Brasil.

6.1.3.2. Para a entrega de sua chave pública à AC-RFB, encarregada da emissão de seu certificado, a AC solicitante faz uso do padrão PKCS#10. Essa entrega é feita por representante legalmente constituído da AC subordinada, em data e hora previamente estabelecida pela AC-RFB.

6.1.4 Disponibilização de chave pública da AC-RFB para usuários

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

- 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];
- Diretório;
- Página *web* da AC-RFB (http://www.receita.fazenda.gov.br/acrfb;
- Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1. Não se aplica

6.1.5.2. O tamanho das chaves criptográficas associadas a certificados emitidos pela AC-RFB será de 4096 (quatro mil e noventa e seis) bits, conforme estabelecido para chaves criptográficas associadas a certificados de AC, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], para os certificados emitidos pela AC-RFB a partir da sua versão 3 (AC-RFBv3).

6.1.5.3. Para os certificados emitidos pelas AC-SRF v1 e AC-RFB v2, o tamanho das chaves criptográficas associadas aos certificados foi de 2048 (dois mil e quarenta e oito) bits.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC-RFB seguem o padrão Homologação da ICP-Brasil NSH-3, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]

6.1.7 Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave segue o padrão “Homologação da ICP-Brasil NSH-3”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8 Geração de chave por *hardware ou software*

6.1.8.1. O processo de geração do par de chaves da AC-RFB é feito por hardware criptográfico com padrão de segurança “Homologação da ICP-Brasil NSH-3”, definido no documento PADROES E ALGORITMOS CRIPTOGRAFICOS DA ICP-BRASIL[9].

6.1.8.2. Não se aplica

6.1.9 Propósitos de uso de chave (conforme campo “Key usage” na X.509 v3)

6.1.9.1 A chave privada da AC Subseqüente é utilizada apenas para a assinatura dos certificados por ela emitidos e para assinatura de sua LCR.

6.1.9.2 A chave privada da AC-RFB é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2 PROTEÇÃO DA CHAVE PRIVADA

A chave privada da AC-RFB é gerada, armazenada e utilizada apenas em hardware criptográfico com padrão de segurança “Homologação da ICP-Brasil NSH-3”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], não havendo, portanto, tráfego da mesma em nenhum momento.

6.2.1 Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC-RFB adota o padrão “Homologação da ICP-Brasil NSH-3”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. O padrão requerido para os módulos de geração de chaves criptográficas das AC de nível imediatamente subseqüente ao da AC-RFB está 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-RFB é dividida em “9” (nove) partes e distribuídas por “9” (nove) custodiantes designados pela AC-RFB (m).

6.2.2.2. É necessária a presença de “3” (três) custodiantes (n), formalmente designados pela AC-RFB, para a ativação do componente e a conseqüente utilização da chave privada.

6.2.3 Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, 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.

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-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-RFB não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.

6.2.4.4. A cópia de segurança deve ser armazenada, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1. As chaves privadas das AC subordinadas à AC-RFB não são arquivadas pela AC-RFB .

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-RFB é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7 Método de ativação de chave privada

A ativação da chave privada da AC-RFB é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de “3” de “9” dos *custodiantes* da chave de ativação da chave criptográfica.

6.2.8 Método de desativação de chave privada

A chave privada da AC-RFB, armazenada em módulo criptográfico, é desativada quando não mais é necessária através 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 cartões criptográficos, protegidos com senha, após a identificação de “3” de “9” dos detentores da chave de ativação da chave criptográfica.

6.2.9 Método de destruição de chave privada

Quando a chave privada da AC-RFB for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, será sobrescrito. Todas as cópias de segurança da chave privada da AC-RFB e todos os cartões criptográficos dos custodiantes serão destruídos.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A AC-RFB armazena as chaves públicas da própria AC-RFB e dos titulares de certificados das AC subseqüentes, bem como as LCR emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1. A chave privada da AC-RFB e dos titulares de certificados por ela emitidos, são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC-RFB pode ser utilizada durante todo

o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. Os certificados emitidos pela AC-RFB para as AC de nível imediatamente subseqüente ao seu terão validade de, no máximo, 8 anos.

6.3.2.4. O período máximo de validade admitido para certificados desta AC é de 10 anos.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes, estão descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 Geração e instalação dos dados de ativação

6.4.1.1. A AC-RFB garante que os dados de ativação da sua chave privada são únicos e aleatórios.

6.4.1.2. Não se aplica.

6.4.2 Proteção dos dados de ativação.

6.4.2.1. Os dados de ativação são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha, e são armazenados no mínimo em ambiente de nível 6 de segurança.

6.4.2.2. Não se aplica.

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-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 gerais de segurança computacional dos equipamentos utilizados para a geração dos pares de chaves criptográficas das AC titulares de certificados emitidos pela AC-RFB, devem ser os mesmos descritos no item abaixo para os computadores servidores da AC-RFB.

6.5.1.3. Os computadores servidores, utilizados pela AC-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-RFB;
b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC-RFB;
c) Acesso restrito aos bancos de dados da AC-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-RFB;
f) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
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. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC-RFB, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC-RFB. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC-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-RFB aplica configurações de segurança definida como EAL3, baseada na *Common Criteria*, que disponibiliza as atualizações deste sistema operacional utilizado nos servidores do Sistema de Certificação Digital.

6.5.3 Controle de segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.

6.5.3.2. Não se aplica.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 Controles de desenvolvimento de sistemas

6.6.1.1. A AC-RFB adota o Sistema de Gerência de Certificados (SGC) – na versão YWYRA. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e, após concluídos os testes, são colocadas em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do CCD avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2 Controle de gerenciamento de segurança

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

a) 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;
b) A AC-RFB opera em equipamento offline para geração, emissão de LCR e assinatura de certificados. Este ambiente não necessita de configuração de segurança de rede.

6.6.2.2. O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC-RFB, envolve o teste 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 a nível de certificados, páginas *web*, scripts etc;
c) Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos;
d) Instalação de novos serviços na plataforma de processamento.

6.6.3 Classificação de segurança de ciclo de vida

Este item não se aplica.

6.6.4 Controles na geração de LCR

Antes de publicadas, todas as LCR geradas pela AC são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número de 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 Os controles implementados para garantir a confidencialidade, integridade e disponibilidade dos serviços da AC-RFB, no site http://www.receita.fazenda.gov.br/acrfb são os seguintes:

a) Infraestrutura de conectividade, incluindo:
   i. alojamento seguro de equipamento de comunicação;
   ii. firewall seguro e serviços de roteador;
   iii. serviço de LAN seguro;
   iv. serviço back office seguro; e
   v. serviço de internet seguro e redundante.

b) Prevenção incidente e avaliação, incluindo,
   i. descoberta de intrusão;
   ii. análise de vulnerabilidade;
   iii. configuração segura de servidor; e
   iv. auditorias técnicas.
   v. administração de Infraestrutura, incluindo
   vi. monitoramento de servidor;
   vii. monitoramento de rede;
   viii. monitoramento de URL; e
   ix. relatórios de largura da banda.

6.7.1.2 Nos servidores e elementos de infraestrutura e proteção de rede utilizados pela AC-RFB, somente os serviços estritamente necessários são habilitados.

6.7.1.3 Os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), que atendem o segmento de rede dos servidores web do sistema de certificação da AC-RFB, estão localizados e operam em ambiente protegido por três perímetros de segurança: os dois primeiros controlados por vigilantes e o terceiro constituído por controle de acesso biométrico.

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

desenvolvimento e homologação.

6.7.1.5 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 permitam 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* estão 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" (ZDM) – em relação aos equipamentos com acesso exclusivamente interno à AC-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 tem capacidade de reconhecer ataques em tempo real e responde-los automaticamente, com medidas tais como: enviar *traps SNMP*, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

6.7.3.2. O sistema de detecção de intrusão tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de 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 – deverão ser registradas em arquivos para posterior análise, que poderá automatizada. A freqüência de exame dos arquivos de registro deverá ser, no mínimo, diária e todas as ações tomadas em decorrência desse exame deverão ser documentadas.

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

O módulo criptográfico utilizado pela AC-RFB para o armazenamento de sua chave privada implementa as características de segurança do padrão “Homologação da ICP-Brasil NSH-3”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
b) a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

7. PERFIS DE CERTIFICADO E LCR

7.1 DIRETRIZES GERAIS

7.1.1. Nos seguintes itens são descritos os aspectos dos certificados e LCR emitidos pela AC-RFB.

7.1.2. Não se aplica.

7.1.3. A AC-RFB especifica, nos itens seguintes, o formato dos certificados emitidos para as AC subseqüentes.

7.2 PERFIL DO CERTIFICADO

Todos os certificados emitidos pela AC-RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.2.1 Número(s) de versão

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

7.2.2 Extensões de certificados

7.2.2.1 Para certificados emitidos pela AC-SRF v1:

Os certificados emitidos pela AC-SRF v1 obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

a) "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o *hash* SHA-1 da chave pública da AC-SRF v1;

b) "*Subject Key Identifier*", não crítica: contém o *hash* SHA-1 da chave pública da AC titular do certificado;

c) "*Key Usage*", crítica: somente os bits keyCertSign e CRLSign são ativados;

d) "*Certificate Policies*", não crítica:

   i. O campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;

   ii. O campo policyQualifiers contém o endereço *URL* da página *web,* http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf, onde se obtém a DPC da AC.

e) O "Basic Constraints", crítica: contém o campo CA=TRUE;

f) "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *web,* http://www.receita.fazenda.gov.br/acsrf/acsrf.crl, onde se obtém a LCR da AC.

7.2.2.2 Para certificados emitidos pela AC-RFB v2:

Os certificados emitidos pela AC-RFB v2 obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

a) "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o *hash* SHA-1 da chave pública da AC-RFB v2;

b) "*Subject Key Identifier*", não crítica: contém o *hash* SHA-1 da chave pública da AC titular do certificado;

c) "*Key Usage*", crítica: somente os bits keyCertSign e CRLSign são ativados;

d) "*Certificate Policies*", não crítica:

   i. O campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;

   ii. O campo policyQualifiers contém o endereço *URL* da página *web,* http://www.receita.fazenda.gov.br/acrfb/dpcacrfb.pdf, onde se obtém a DPC da AC.

e) O "Basic Constraints", crítica: contém o campo CA=TRUE;

f) "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *web* http://www.receita.fazenda.gov.br/acrfb/acrfb.crl, onde se obtém a LCR da AC.

7.2.2.3 Para certificados emitidos pela AC-RFB v3:

Os certificados emitidos pela AC-RFB v3 obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

a) "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o *hash* da chave pública da AC-RFB v3;

b) "*Subject Key Identifier*", não crítica: contém o *hash* da chave pública da AC titular do certificado;

c) "*Key Usage*", crítica: somente os bits keyCertSign e CRLSign são ativados;

d) "*Certificate Policies*", não crítica:

   i. O campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;

   ii. O campo policyQualifiers contém o endereço *URL* da página *web,* http://www.receita.fazenda.gov.br/acrfb/dpcacrfb.pdf, onde se obtém a DPC da AC.

e) O "Basic Constraints", crítica: contém o campo CA=TRUE;

f) "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *web* http://www.receita.fazenda.gov.br/acrfb/acrfbv3.crl, onde se obtém a LCR da AC.

A AC-RFB v3 implementa também a seguinte extensão, definidas como opcional pela ICP-Brasil:

a) "*Authority Information Access*", não critica, contendo o endereço na web onde se obtém o arquivo P7B com certificados da cadeia;

- http://www.receita.fazenda.gov.br/cadeias/acrfbv3.p7b
- (OID = 1.3.6.1.5.5.7.1.1).

7.2.3 Identificadores de algoritmos

Os certificados emitidos pela AC-SRF v1 e AC-RFB v2 são assinados com o uso do algoritmo RSA com SHA-1 como função *hash* (OID = 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

Os certificados emitidos pela AC-RFB v3 são assinados com o uso do algoritmo sha512WithRSAEncryption como função *hash*, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

7.2.4 Formatos de nome

Para os certificados emitidos pela AC-RFB, o nome da AC titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C= BR
O= ICP-Brasil
OU= Secretaria da Receita Federal do Brasil - RFB
CN= nome da AC

7.2.5 Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC-RFB são as seguintes:

a) Não serão utilizados sinais de acentuação, tremas ou cedilhas;
b) Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.2.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC-RFB após conclusão do processo de seu credenciamento, é **2.16.76.1.1.8**.

7.2.7 Uso da extensão “Policy Constraints”

Não se aplica

7.2.8 Sintaxe e semântica dos qualificadores de política

7.2.8.1 Para a AC-SRF v1:

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço *web* http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf.

7.2.8.2 Para a AC-RFB v2 e v3:

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço *web* http://www.receita.fazenda.gov.br/acrfb/dpcacrfb.pdf.

7.2.9 Semântica de processamento para extensões criticas

Extensões críticas são interpretadas, no âmbito da AC-RFB, conforme a RFC 5280.

7.3 PERFIL DE LCR

7.3.1 Número (s) de versão

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

7.3.2 Extensões de LCR e de suas entradas

7.3.2.1. A AC-RFB adota todas as extensões de LCR definidas como obrigatórias pela ICP-Brasil.

7.3.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

a) **“*Authority Key Identifier*”, não crítica:** deve conter o *hash* da chave pública da AC que assina a LCR;
b) **“*CRL Number*”, não crítica**: deve conter um número seqüencial para cada LCR emitida.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração nesta DPC da AC-RFB será submetida previamente à aprovação do CG da ICP-Brasil. A DPC será alterada sempre que a legislação assim o exigir.

8.2 POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO

A AC-RFB publica esta DPC, em sua página *web* acessível pela URL, http://www.receita.fazenda.gov.br/acrfb/dpcacrfb.pdf. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na *web*.

8.3 PROCEDIMENTOS DE APROVAÇÃO

Essa DPC foi submetida à aprovação, durante o processo de credenciamento da AC-RFB**,** conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9. DOCUMENTOS REFERENCIADOS

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

Ref	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[4]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NAICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[3]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09

9.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, 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 Instruções Normativas que os aprovaram.

Ref	**Nome do documento**	**Código**
[2]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

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

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