Declaração de Práticas de Certificação da Autoridade Certificadora Safeweb RFB

DPC - AC SAFEWEB RFB

Versão 2.0

Novembro 2017

AC SAFEWEB RFB

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou alteração	Item alterado
1.0	10/12/2014	N/A	N/A
1.1	28/04/2015	DOC-ICP-05	4.8.1, 7.3.2.2 “c”, 5.1.2.1.14
1.2	20/10/2015	Resolução 107, de 25/08/2015	3.1.1.1 “a”
		Resolução 113, de 30/09/2015	3.2.2 “b” e “c”
2.0	27/11/2017	DOC-ICP-05 e DPC AC RFB	1.3.4.1, 3.1.1.5, 3.1.2.1, 3.1.3, 3.1.8, 3.1.9.2, 3.1.10.1.2, 3.1.10.1.3, 3.1.10.2, 3.1.10.2 “a”, 3.1.11, 3.4, 4.3.2, 4.4.1.2 “f”, “g” e “h”, 4.4.15.2, 6.1.7, 6.1.9, 6.2, , 6.2.1.2, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.3.1, 6.3.2.4, 6.4.1.1, 6.5.1.6, 6.5.2, 6.5.3.2, 8.3, 9.1, 9.2 e 9.3
		Resolução 114, de 30/09/2015	3.1.1.1 “a”, 3.1.1.7, 3.1.9, 3.1.9.1
		Resolução 115, de 11/11/2015	3.1.1.8, 3.1.1.4.1, 3.1.12, 4.4.2
		Resolução 116, de 09/12/2015	6.1.1.2, 6.1.6, 6.1.8.1, 6.1.8.2, 6.2.1.1, 6.2.1.3, 6.2.4.3, 6.8.1, 6.8.2
		Resolução 118, de 09/12/2015	2.6.4.1, 7.3.2.2 “a” e “c”
		DOC-ICP-05 e DOC-ICP-01.02	1.3.4.4, 3.1.5, 3.4, 6.1.1.2
		N/A	1.3.1.1, 1.3.2.1, 1.3.3.1, 1.3.4.4, 1.4, 2.3.2, 2.6.1, 2.6.4, 2.6.1.1, 2.8.4.1, 3.1.5, 3.4, 4.4.3.1, 6.1.1.2, 6.1.1.3, 6.1.4 “c”, 6.2.1.2, 8.2

1 INTRODUÇÃO

1.1 VISÃO GERAL

Esta Declaração de Práticas de Certificação - DPC constitui os requisitos mínimos, obrigatoriamente observados pela Autoridade Certificadora Safeweb RFB – AC Safeweb RFB, integrante da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil e descreve as práticas e os procedimentos utilizados pela AC Safeweb RFB na execução de seus serviços.

Esta DPC adota a mesma estrutura utilizada no DOC-ICP-05, que estabelece os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10].

1.2 IDENTIFICAÇÃO

Este documento é chamado “Declaração de Práticas de Certificação da AC Safeweb RFB”, referido a seguir simplesmente como "DPC - AC Safeweb RFB" e descreve as práticas e os procedimentos empregados pela AC Safeweb RFB no âmbito da ICP-Brasil.

O OID da DPC - AC Safeweb RFB, atribuído pela AC Raiz após conclusão do seu processo de credenciamento, é **2.16.76.1.1.64.**

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 AUTORIDADE CERTIFICADORA - AC

1.3.1.1 DADOS DA AUTORIDADE CERTIFICADORA

Esta DPC se refere à AC Safeweb RFB e encontra-se publicada em sua página web www.safeweb.com.br.

A AC Safeweb RFB está no nível imediatamente subsequente ao da Autoridade Certificadora da Secretaria da Receita Federal do Brasil - AC RFB, que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira - AC Raiz.

Com relação aos tipos específicos de certificados emitidos pela Autoridade Certificadora Safeweb RFB, devem ser observadas as Políticas de Certificado da AC Safeweb RFB, que explicam como os certificados são gerados, administrados pela AC Safeweb RFB e utilizados pela comunidade. Esses documentos estão disponíveis em página web www.safeweb.com.br.

1.3.2 AUTORIDADE DE REGISTRO - AR

1.3.2.1 Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência das Autoridades de Registro - ARs. As Autoridades de Registro vinculadas à AC Safeweb RFB, denominadas de ARs vinculadas, estão relacionadas na página: www.safeweb.com.br que contém as seguintes informações:

a) relação de todas as ARs credenciadas, com informações sobre as PCs que praticam;

b) para cada AR credenciada, relação dos endereços de todas as instalações técnicas, autorizadas a funcionar pela AC Raiz;

c) para cada AR credenciada, relação de eventuais postos provisórios autorizados a funcionar pela AC Raiz, com data de criação e encerramento de atividades;

d) relação de AR que tenha se descredenciado da cadeia da AC, com respectivas datas do descredenciamento;

e) relação de instalações técnicas de AR credenciada, que tenham deixado de operar, com respectivas datas de encerramento das atividades;

f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICP-Brasil, se for o caso.

1.3.2.2. A AC Safeweb RFB mantém as informações acima sempre atualizadas.

1.3.3 PRESTADOR DE SERVIÇOS DE SUPORTE – PSS

1.3.3.1 Os Prestadores de Serviços de Suporte vinculados à AC Safeweb RFB estão relacionados na página www.safeweb.com.br.

1.3.3.2 PSS são entidades utilizadas pela AC Safeweb RFB ou pelas AR Vinculadas para desempenhar atividade descrita nesta DPC e/ou na PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.4 TITULARES DE CERTIFICADO

1.3.4.1 Podem ser titulares de certificados emitidos pela AC SAFEWEB RFB pessoas físicas inscritas no CPF, desde que não enquadradas na situação cadastral de CANCELADA ou NULA, e pessoas jurídicas inscritas no CNPJ, desde que não enquadradas na condição de INAPTA, SUSPENSA, BAIXADA, NULA ou CANCELADA, conforme o disposto nos incisos I e II do art. 6° da Instrução Normativa RFB n° 222, de 11 de Outubro de 2002.

1.3.4.2 Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será o detentor da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrada no CNPJ da RFB.

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

1.3.4.4 Não se aplica.

1.3.5 APLICABILIDADE

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

Política de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da AC Safeweb RFB	PC AC Safeweb RFB A1	2.16.76.1.2.1.51
Política de Certificado de Assinatura Digital tipo A3 da AC Safeweb RFB	PC AC Safeweb RFB A3	2.16.76.1.2.3.48

As PCs correspondentes estão relacionadas às aplicações para as quais são adequados os certificados emitidos pela AC Safeweb RFB e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

1.4 DADOS DE CONTATO

Dúvidas decorrentes da leitura desta DPC - AC Safeweb RFB e que não sejam respondidas mediante a leitura da página www.safeweb.com.br podem ser esclarecidas contatando:

Setor de Compliance da AC Safeweb RFB

Telefone: (51) 3018-0300

E-mail: compliance@safeweb.com.br

Safeweb Segurança da Informação Ltda.

Endereço: Av. Princesa Isabel, 828 – Porto Alegre/RS – CEP 90620-000

2 DISPOSIÇÕES GERAIS

2.1 OBRIGAÇÕES E DIREITOS

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

2.1.1 OBRIGAÇÕES DA AUTORIDADE CERTIFICADORA SAFEWEB RFB

As obrigações da AC Safeweb RFB são as abaixo relacionadas:

a) operar de acordo com esta DPC - AC Safeweb RFB e com as PCs que pratica;

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

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC RFB, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;

e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou encerramento de suas atividades;

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados de usuários finais e de ARs vinculadas;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas Listas de Certificados Revogados - LCR e, quando aplicável, disponibilizar consulta *on-line* de situação do certificado (OCSP - *Online Certificate Status Protocol*);

k) publicar em sua página web sua DPC - AC Safeweb RFB e as PCs aprovadas que implementa;

l) publicar, em sua página web, as informações definidas no item 2.6.1.2 deste documento;

m) publicar, em sua 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 Comitê Gestor da ICP-Brasil;

p) adotar as medidas de segurança e controle previstas na DPC-AC Safeweb RFB, nas Políticas de Certificado e de Segurança implementadas, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil e da Secretaria da Receita Federal do Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e da Secretaria da Receita Federal do Brasil 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;

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 ARs vinculadas, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do Comitê Gestor da ICP-Brasil;

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

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

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

x) atender à Instrução Normativa nº. 222 da Secretaria da Receita Federal do Brasil, de 11 de outubro de 2002, nos seus artigos 10º e 11º.

2.1.2 OBRIGAÇÕES DAS AUTORIDADES DE REGISTRO – AR

As obrigações das ARs vinculadas 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 Safeweb RFB

utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP BRASIL [1];

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

e) disponibilizar os certificados emitidos pela AC Safeweb 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 Safeweb RFB e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];

h) manter e garantir a segurança da informação por ela 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 e 3.1.11;

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

Constituem-se obrigações do titular de certificado emitido pela AC Safeweb RFB:

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

b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;

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

e) informar à AC Safeweb RFB qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;

f) pagar o preço do processo de emissão do certificado;

g) responsabilizar-se por todos os atos praticados com utilização do referido certificado e sua correspondente chave privada;

h) utilizar obrigatoriamente senha para proteção da chave privativa;

i) obedecer estritamente a esta DPC - AC Safeweb RFB e as PCs aplicáveis, bem como respeitar a legislação vigente, incluindo, mas não se limitando, as regras definidas pelo CG da ICP-Brasil e as obrigações contratuais assumidas perante a AC Safeweb RFB e a AR que esteja vinculada.

NOTA: Em se tratando de certificado emitido para pessoa jurídica estas obrigações também 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:

i. não constar da LCR da AC emitente;

ii. não estiver expirado; e

iii. puder ser verificado com o uso de certificado válido da AC emitente.

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

2.1.5 OBRIGAÇÕES DO REPOSITÓRIO DA AC SAFEWEB RFB

As obrigações da AC Safeweb RFB em relação ao seu repositório são:

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

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

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

2.2 RESPONSABILIDADES

2.2.1 RESPONSABILIDADES DA AC SAFEWEB RFB

2.2.1.1 A AC Safeweb RFB responde pelos danos a que der causa.

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

2.2.2 RESPONSABILIDADES DAS AUTORIDADES DE REGISTRO VINCULADAS

2.2.2.1 A AR Vinculada será responsável pelos danos a que der causa.

2.3 RESPONSABILIDADE FINANCEIRA

2.3.1 INDENIZAÇÕES DEVIDAS PELA TERCEIRA PARTE - *Relying Party*

A terceira parte - *Relying Party* - não é responsável perante a AC Safeweb RFB e AR a ela vinculada, exceto na hipótese de prática de ato ilícito. Nesse caso, essa terceira parte responderá em quaisquer esferas de direito, e deverá indenizar a AC Safeweb RFB e/ou os titulares de seus certificados pelos danos a que der causa em decorrência de omissão ou ação não conforme com a legislação aplicável.

2.3.2 RELAÇÕES FIDUCIÁRIAS

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

Os detalhes das condições de aplicação da Política de Garantia estão disponíveis na página web www.safeweb.com.br.

2.3.3 PROCESSOS ADMINISTRATIVOS

O titular do certificado que julgar-se prejudicado em decorrência do uso do certificado digital terá o direito de comunicar à AC Safeweb RFB que deseja a indenização prevista no documento Política de Garantia. Serão observadas as seguintes condições:

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC Safeweb RFB, tal comprometimento deverá ter sido provado por perícia realizada por perito especializado e independente, escolhido em consenso;

b) nos casos de erro na transcrição, o titular do certificado não poderá requerer qualquer indenização quando houver aceito o certificado.

2.4 INTERPRETAÇÃO E EXECUÇÃO

2.4.1 LEGISLAÇÃO

Esta DPC é regida pela Medida Provisória nº 2.200-02, pelas Resoluções do Comitê Gestor da ICP-Brasil, bem como pelas demais leis em vigor no Brasil.

2.4.2 FORMA DE INTERPRETAÇÃO E NOTIFICAÇÃO

2.4.2.1 Caso esta DPC - AC Safeweb RFB ou alguma de suas disposições venha a ser considerada ou declarada inválida, ilegal ou não aplicável por lei, a AC Safeweb RFB tomará de imediato às medidas necessárias para adequar esta DPC ou a disposição em questão às exigências legais.

2.4.2.2 As notificações, solicitações ou quaisquer outras comunicações necessárias serão realizadas pela AC Safeweb RFB e pelas ARs vinculadas por mensagem eletrônica (*e-mail*) a ser enviada para o endereço eletrônico fornecido pelo solicitante no formulário de solicitação. A mensagem eletrônica (*e-mail*) será considerada como recebida quando enviado a esse endereço.

2.4.3 PROCEDIMENTO DE SOLUÇÃO DE DISPUTA

2.4.3.1 Em caso de conflito entre esta DPC - AC Safeweb RFB e outras declarações, políticas, planos, acordos, contratos ou documentos, esta DPC - AC Safeweb RFB prevalecerá.

2.4.3.2 Esta DPC - AC Safeweb RFB não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil e da Secretaria da Receita Federal do Brasil.

2.4.3.3 Os casos omissos deverão ser encaminhados para apreciação da AC Raiz.

2.5 TARIFAS DE SERVIÇOS

Pelo certificado emitido será cobrado o valor estabelecido contratualmente.

2.5.1 TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS

Pela emissão e renovação do certificado será cobrado o valor estabelecido contratualmente.

2.5.2 TARIFAS DE ACESSO AO CERTIFICADO

Pelo acesso ao certificado será cobrado o valor estabelecido contratualmente.

2.5.3 TARIFAS DE REVOGAÇÃO OU DE ACESSO A INFORMAÇÃO DE STATUS

Não há tarifas previstas pela AC Safeweb RFB para a revogação. Pelo acesso a informação de status a tarifa é variável conforme definição interna da AC Safeweb RFB.

2.5.4 TARIFAS PARA OUTROS SERVIÇOS

Para outros serviços será cobrado o valor estabelecido contratualmente.

2.5.5 POLÍTICA DE REEMBOLSO

Na hipótese de necessidade de o certificado ser revogado por motivo de comprometimento da chave privada da AC Safeweb RFB ou da mídia armazenadora da chave privada da AC Safeweb RFB, ou ainda quando constatada a emissão imprópria ou defeituosa, com culpa da AC Safeweb RFB, será emitido outro certificado em substituição, sem cobrança ao titular do mesmo. Não haverá reembolso no caso de emissão sem custo de outro certificado em substituição.

2.6 PUBLICAÇÃO E REPOSITÓRIO

2.6.1 PUBLICAÇÃO DE INFORMAÇÃO DA AC SAFEWEB RFB

2.6.1.1 A AC Safeweb RFB publica e mantém disponível em seu site www.safeweb.com.br informações com disponibilidade mínima de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2 As seguintes informações, no mínimo, são publicadas pela AC Safeweb RFB em página web:

a) Seu próprio certificado;

b) Suas LCRs;

c) Sua DPC - AC Safeweb RFB;

d) As Políticas de Certificado – PC, que pratica;

e) Uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;

f) Uma relação, regularmente atualizada, das ARs vinculadas que tenham celebrado acordos operacionais com outras ARs da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e

g) Uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2 FREQUÊNCIA DE PUBLICAÇÃO

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

2.6.3 CONTROLES DE ACESSO

Somente os funcionários competentes e designados especialmente para esse fim poderão alterar as informações constantes nesta DPC - AC Safeweb RFB e nas suas Políticas de Certificados que pratica, depois de autorizado pelo Comitê Gestor da ICP-Brasil.

Somente a AC Safeweb RFB, por seus funcionários competentes e designados especialmente para esse fim, pode efetuar as necessárias atualizações de sua LCR. Caso se faça necessário modificar os dados contidos nos certificados, será necessária a revogação dos certificados. Não há restrições para leitura desta DPC - AC Safeweb RFB, das PCs que implementa e das LCRs.

Todas as informações disponibilizadas pela AC Safeweb RFB, conforme o item 2.6.1 desta DPC - AC Safeweb RFB, estão disponíveis para leitura sem restrições.

2.6.4 REPOSITÓRIOS

Os repositórios da AC Safeweb RFB são acessados, utilizando o protocolo de acesso http ou https, através da página http://www.safeweb.com.br/ac/repositorio. Os repositórios estão disponíveis em no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. Os repositórios obedecem aos requisitos de segurança estabelecidos no item 5 desta DPC.

2.6.4.1 A AC Safeweb RFB disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR.

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 das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.2 As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por

meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

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

2.7.4 A AC Safeweb RFB recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5 A AC Safeweb RFB e as entidades da ICP-Brasil a ela diretamente vinculadas – AR Vinculadas e PSS, receberam auditoria prévia, para fins de credenciamento, sendo a AC Safeweb RFB responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8 SIGILO

2.8.1 DISPOSIÇÕES GERAIS

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

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

2.8.1.3 Não se aplica.

2.8.2 TIPOS DE INFORMAÇÕES SIGILOSAS

2.8.2.1 Todas as informações coletadas, geradas, transmitidas e mantidas pela AC Safeweb RFB e pelas ARs vinculadas são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3.

Essas informações serão arquivadas de acordo com sua classificação, especificada na Política de Segurança.

2.8.2.2 Como princípio geral, nenhum documento, informação ou registro fornecido à AC Safeweb RFB ou à AR Vinculada deve ser divulgado.

2.8.3 TIPOS DE INFORMAÇÕES NÃO SIGILOSAS

Não são consideradas como informações sigilosas pela AC Safeweb RFB e pela AR Vinculada:

a) os certificados e as LCR emitidos pela AC Safeweb RFB;

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

c) as PCs praticadas pela AC Safeweb RFB;

d) esta DPC - AC Safeweb RFB;

e) as versões públicas de Políticas de Segurança;

f) a conclusão dos relatórios de auditoria.

A AC Safeweb RFB e a AR Vinculada julgam confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) o solicitante autorize formalmente a sua divulgação;

b) depois de entregue pelo solicitante, os dados sejam obtidos ou possam ter sido obtidos legalmente de terceiro (s) sem quaisquer restrições;

c) tenham a exibição ordenada por determinação judicial ou autoridade competente com poder de polícia; se possível, a exigência poderá ser comunicada de imediato ao solicitante.

Os motivos que justificaram a não emissão de um certificado poderão ser mantidos confidenciais pela AC Safeweb RFB e pela AR Vinculada, salvo na hipótese da alínea "c".

2.8.4 DIVULGAÇÃO DE INFORMAÇÃO DE REVOGAÇÃO DE CERTIFICADO

2.8.4.1 A AC Safeweb RFB disponibiliza permanentemente em seu site www.safeweb.com.br, com atualização definida nas correspondentes PCs, relação de certificados por ela emitidos que foram revogados.

2.8.4.2 Os motivos que justificaram a revogação são sempre informados ao titular ou responsável pelo certificado e mantidos confidenciais pela AC Safeweb RFB e pela AR Vinculada, exceto quando o titular do certificado revogado solicitar ou autorizar expressamente a sua divulgação a terceiros, ou quando tais motivos sejam requisitados por determinação judicial ou de

autoridade competente, caso em que a AC Safeweb RFB ou a AR Vinculada, se estiver obrigada a divulgá-los, poderá comunicar previamente ao titular do certificado a existência de tal determinação.

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

As informações fornecidas pelo solicitante ou titular do certificado, bem como os documentos e registros relativos ao solicitante, ao titular do certificado, à solicitação ou ao certificado emitido não são mantidos sob sigilo pela AC Safeweb RFB ou pela AR Vinculada quando a lei prevê a sua publicidade e/ou divulgação ou por ordem judicial ou de autoridade competente.

2.8.6 INFORMAÇÕES A TERCEIROS

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC Safeweb RFB ou das ARs vinculadas, será fornecido a terceiros, exceto quando o requerente o solicite por meio 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 A qualquer tempo o titular do certificado, ou seu mandatário, terá acesso aos dados que lhe dizem respeito e que estejam sob a guarda da AC Safeweb RFB e das ARs Vinculadas.

2.8.7.2 Qualquer liberação de informação pela a AC Safeweb RFB ou pelas ARs Vinculadas somente será permitida mediante autorização formal do titular do certificado. Essa autorização pode ser feita no ato da solicitação do certificado, no próprio formulário de solicitação, ou posteriormente, por documento legalmente aceito.

2.8.8 OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO

A AC Safeweb RFB e as ARs Vinculadas podem divulgar informações que não sejam consideradas sigilosas pelo fato de:

a) estarem na posse legítima da AC Safeweb RFB ou das ARs Vinculadas antes de seu fornecimento pelo solicitante ou titular do certificado;

b) depois do seu fornecimento pelo solicitante ou titular do certificado, terem sido obtidas ou puderem ter sido obtidas legalmente de um terceiro;

c) terem sido requisitadas por determinação judicial ou governamental ou de autoridade competente; A AC Safeweb RFB nesse caso, se possível, comunicará previamente e de imediato o solicitante ou titular do certificado a existência de tal determinação.

2.9 DIREITOS DE PROPRIEDADE INTELECTUAL

A emissão do certificado não implica a transferência, cessão ou licença de direitos de propriedade intelectual de softwares, certificados, políticas, especificações de práticas e procedimentos, nomes, chaves criptográficas e outros da AC Safeweb RFB ou de AR vinculadas para o solicitante.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 REGISTRO INICIAL

3.1.1 DISPOSIÇÕES GERAIS

3.1.1.1 As ARs Vinculadas à AC Safeweb RFB utilizam os seguintes requisitos e procedimentos para 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 indivíduo), 3.1.10 (autenticação da identidade de uma organização) desta DPC, podendo ser realizada simultaneamente por dois agentes de registro:

I – Confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como a sua representante é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo previr expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública, com poderes específicos para atuar perante a ICP-Brasil e com prazo de validade de até 90 (noventa) dias. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim.

II – Confirmação da identidade de uma organização: comprovação de que os documentos

apresentados referem-se, efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;

III – Emissão do certificado: conferência dos dados da solicitação do certificado com os constantes nos documentos apresentados e liberação da emissão do certificado no sistema da AC.

b) VERIFICAÇÃO DA SOLICITAÇÃO – confirmação da validação realizada observando que deve ser executada, obrigatoriamente:

I – Por agente de registro distinto do que executou a etapa de validação;

II – Em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;

III – Somente após o recebimento, na instalação técnica da AR, de cópia da documentação apresentada na etapa de validação;

IV – Antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.1.1.2 O processo de validação ao ser realizado pelo agente de registro fora do ambiente físico da AR, deverá utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR.

3.1.1.3 Todas as etapas dos processos de validação e verificação da solicitação do certificado devem ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC Safeweb RFB, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. Tais registros devem feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

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

3.1.1.4.1 Não se aplica.

3.1.1.5 Não se aplica.

3.1.1.6 Não se aplica.

3.1.1.7 A AC Safeweb RFB disponibiliza, para todas as AR vinculadas a sua respectiva cadeia, através de sistema (Gedar), uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

3.1.1.8 Não se aplica.

3.1.2 TIPOS DE NOMES

3.1.2.1 A AC Safeweb RFB emite certificados com nomes que possibilitam determinar a identidade da pessoa ou organização a que se referem. Para tanto utiliza o "*distinguished name*" do padrão ITU X.500, endereços de correio eletrônico, endereços de página Web (URL), entre outras informações que permitam a identificação do titular.

3.1.2.2 Não se aplica.

3.1.3 NECESSIDADE DE NOMES SIGNIFICATIVOS

A AC Safeweb RFB faz uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem, para a identificação dos titulares dos certificados emitidos pela AC Safeweb RFB.

Para certificados de pessoa física (e-CPF), o campo *Common Name* é composto do nome do Titular do Certificado, conforme consta no Cadastro de Pessoa Física - CPF.

Para os certificados de pessoa jurídica (e-CNPJ), o campo *Common Name* é composto do nome empresarial da pessoa jurídica, conforme consta no Cadastro Nacional de Pessoa Jurídica – CNPJ.

3.1.4 REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES

Não se aplica.

3.1.5 UNICIDADE DE NOMES

Os identificadores do tipo "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC Safeweb RFB. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo. Para assegurar a unicidade do campo, no certificado de pessoa física (e-CPF) é incluído o número do CPF após o nome do titular do certificado e, no certificado de pessoa jurídica (e-CNPJ), é incluído o número do CNPJ.

3.1.6 PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

Para a AC Safeweb RFB não há disputa de nomes entre solicitantes de certificados, uma vez que o nome será obtido a partir dos dados da RFB, CPF ou CNPJ para certificados de pessoa física ou jurídica, respectivamente, acrescido do número de inscrição, o que garante a unicidade de todos os nomes no âmbito da AC Safeweb RFB.

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 de 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 é realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

3.1.9.1 DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

Durante a solicitação dos certificados e-CPF é realizada consulta da situação cadastral do solicitante mediante número de CPF cadastrado através da RFB e consultado nesta base, conforme art. 6º da Instrução Normativa SRF N° 222. Se o CPF informado for inexistente ou se a pessoa física apresentar a condição de CANCELADA ou NULA, a solicitação não será enviada à AC Safeweb RFB.

Deverá ser apresentada a seguinte documentação, em sua versão original, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado:

a) Cédula de Identidade ou Passaporte, se brasileiro;

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

c) Passaporte, se estrangeiro não domiciliado no Brasil;

d) 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 da validação presencial;

e) Comprovante de residência ou domicílio, declarado expressamente em Termo de Titularidade e Responsabilidade e devidamente assinado pelo titular;

f) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11] e;

g) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no

DOC-ICP-05.03 [11].

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: A AC Safeweb RFB reserva-se ao direito de somente aceitar a apresentação da Carteira de Trabalho e Previdência Social (CTPS) em complementação ao primeiro documento de identificação apresentado. A aceitabilidade da CTPS como documento único de identificação para emissão do Certificado Digital deverá passar por análise e parecer da AC.

NOTA 3: 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 do titular no Termo de Titularidade e Responsabilidade, ou declaração emitida por seu empregador.

NOTA 4: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a Carteira Nacional de Habilitação (CNH), Carteira de Trabalho e Previdência Social (CTPS) ou 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 CARACTERÍSTICAS 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: Os documentos que possuem data de validade precisam estar dentro do prazo. CNH vencida não será aceita em hipótese alguma para identificação de titular de certificado digital.

NOTA 9: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

NOTA 10: 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.

NOTA 11: O e-mail de comunicação fornecido, deve ser exclusivo e obrigatório do titular do CD, para garantia da integridade e segurança das informações prestadas.

3.1.9.2 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

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

a) Cadastro de Pessoa Física – CPF;

b) Nome completo, sem abreviações;

c) Data de nascimento;

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

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

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

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

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

e) Número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente;

g) Documento assinado pela empresa com o valor do campo de *login* (UPN), quando aplicável.

3.1.9.2.3 Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original. Deve ser mantido arquivo com as cópias de todos os documentos utilizados.

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

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

3.1.10 AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO

3.1.10.1 DISPOSIÇÕES GERAIS

3.1.10.1.1 A confirmação da identidade de uma pessoa jurídica é feita mediante consulta as bases de dados da RFB.

3.1.10.1.2 Em sendo o titular do certificado pessoa jurídica, será designado o representante legal da pessoa jurídica como responsável pelo certificado, que será o detentor da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica

cadastrado no CNPJ da RFB.

3.1.10.1.3 Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) Apresentação do rol de documentos, em sua versão original, elencados no item 3.1.10.2;

b) Apresentação do rol de documentos, em sua versão original, elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado; e

c) Presença física dos representantes legais e do responsável pelo uso do certificado, 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

Durante a solicitação de certificado e-CNPJ é realizada consulta à situação cadastral do CNPJ junto ao cadastro da RFB. Se o CNPJ estiver INAPTO, SUSPENSO, BAIXADO, NULO ou CANCELADO - situações que impedem o fornecimento do certificado - a solicitação não poderá ser enviada para a AC Safeweb RFB. A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos à sua habilitação jurídica:

I – Se pessoa jurídica criada ou autorizada por lei:

1) Original ou Cópia Autenticada do Ato constitutivo, devidamente registrado no órgão competente; e

2) Consulta impressa e atual do CNPJ;

II – Se entidade privada:

1) Original ou Cópia Autenticada do Ato constitutivo, devidamente registrado no órgão competente; e

2) Documentos 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

3.1.10.3.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

a) Nome empresarial constante do Cadastro Nacional de Pessoas Jurídicas – CNPJ, sem abreviações;

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);

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

d) Data de nascimento do responsável pelo certificado.

3.1.10.3.2 Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado poderá, a seu critério e mediante declaração expressa no termo de titularidade, solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.1.9.2.

3.1.11 AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO, APLICAÇÃO OU CÓDIGO

Não se aplica.

3.1.12 AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTO PARA CERTIFICADO CF-E-SAT

Não se aplica.

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

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

3.2.2 Esse processo será conduzido conforme uma das seguintes possibilidades:

a) Adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado, ou;

b) A solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva, permitida tal hipótese apenas para os certificados digitais de pessoa física.

3.2.3 Não se aplica.

3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO OU EXPIRAÇÃO

3.3.1 Após a revogação ou expiração do certificado, o solicitante pode solicitar um novo certificado, enviando à AR Vinculada uma solicitação, na forma, condições e prazo estabelecidos para a solicitação inicial de um certificado.

3.3.2 Não se aplica.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado é feita através de formulário específico, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados entre a solicitação de revogação e a solicitação de emissão.

Os procedimentos para solicitação de revogação de certificado estão descritos no item 4.4.3.1 desta DPC. As solicitações de revogação de certificados são obrigatoriamente documentadas.

4 REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

4.1.1 A solicitação de emissão de um Certificado Digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR Vinculada. Toda referência a formulário deverá ser entendida também como referência a outras formas que a AR Vinculada possa vir a adotar. Dentre os requisitos e procedimentos operacionais estabelecidos pela AC Safeweb RFB para as solicitações de emissão de certificado, estão:

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

4.1.2 Não se aplica.

4.1.3 Não se aplica.

4.1.4 Não se aplica.

4.2 EMISSÃO DE CERTIFICADO

4.2.1 Depois da validação da solicitação do certificado, de que trata o item 3.1.1.1, a AC Safeweb RFB procede à emissão do certificado. O certificado emitido é inserido na relação de

certificados emitidos pela AC Safeweb RFB. A notificação de emissão é feita por diferentes meios como e-mail contendo o certificado ou e-mail solicitando *download* em url específico ou em mídia.

4.2.2 Certificados do tipo A1 são considerados válidos a partir do momento de sua emissão; certificados do tipo A3 são considerados válidos a partir da data de início de validade nele constante.

4.3 ACEITAÇÃO DO CERTIFICADO

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

4.3.2 A aceitação de todo certificado emitido é declarada implicitamente pelo respectivo titular assim que for utilizado. No caso de certificados emitidos para pessoas jurídicas, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

Ao aceitar um e-CPF, o Titular:

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

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

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

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

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

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

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

4.3.3 Não se aplica.

4.4 REVOGAÇÃO DE CERTIFICADO

4.4.1 CIRCUNSTÂNCIAS PARA REVOGAÇÃO

4.4.1.1 Neste item, a DPC caracteriza as circunstâncias nas quais um certificado poderá ser

revogado.

4.4.1.2 Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;

b) Quando for necessária a alteração de qualquer informação constante no mesmo;

c) No caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora;

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

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

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

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

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

i) Por decisão judicial.

4.4.1.3 Deve-se observar ainda que:

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

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

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

4.4.2 QUEM PODE SOLICITAR A REVOGAÇÃO

A revogação de um certificado somente pode ser solicitada:

a) Por solicitação do titular do certificado;

b) Por solicitação do responsável pelo certificado, no caso de certificado de pessoas jurídicas;

c) Por solicitação de empresa ou órgão, no caso de certificado fornecido por essa empresa ou órgão para seus empregados, funcionários, servidores, parceiros ou fornecedores;

d) Por determinação da AC Safeweb RFB;

e) Por solicitação da AC RFB, do CG da ICP-Brasil ou da AC Raiz, ou;

f) Por solicitação da AR Vinculada que recebeu a solicitação.

4.4.3 PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.4.3.1 Para solicitar a revogação é necessário o envio à AC Safeweb RFB ou à AR vinculada de um formulário disponibilizado pela AC Safeweb RFB no site www.safeweb.com.br, preenchido com qualificações do titular ou responsável pelo certificado, tais como: nome completo, CPF, RG, protocolo, tipo do certificado e a indicação do motivo da solicitação, em caso de pessoa jurídica, indicar também as qualificações da empresa, tais como: razão social, CNPJ, IE, representante legal, CPF e RG. A AC Safeweb RFB garante que todos agentes habilitados podem, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados conforme o item 4.4.2.

4.4.3.2 Como diretrizes gerais:

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

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

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

d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado e com a atualização da situação do certificado nas bases de dados da AC Safeweb RFB de consulta OCSP, quando aplicável.

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

4.4.3.4 Não se aplica.

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

4.4.3.6 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 O prazo máximo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pela AC Safeweb RFB é de 3 (três) dias.

4.4.5 CIRCUNSTÂNCIAS PARA SUSPENSÃO

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

4.4.6 QUEM PODE SOLICITAR SUSPENSÃO

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

4.4.7 PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO

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

4.4.8 LIMITES NO PERÍODO DE SUSPENSÃO

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

4.4.9 FREQUÊNCIA DE EMISSÃO DE LCR

4.4.9.1 Neste item é definida a frequência de emissão da LCR referente a certificados de usuários finais.

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

4.4.9.3 Não se aplica.

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 ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

4.4.11 DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE

O processo de revogação on-line está disponível ao titular do certificado, conforme descrito no item 4.4.3. A AC Safeweb RFB dispõe de recursos para verificação on-line de informações de status de certificados, quando aplicável por força de contratação específica. A verificação poderá ser

realizada diretamente na AC Safeweb RFB, por meio do protocolo *On-line Certificate Status Protocol* – OSCP.

4.4.12 REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE

Não há requisitos específicos para a verificação on-line de informações de revogação de certificados por parte das terceiras partes (*relying parties*).

4.4.13 OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

Não se aplica.

4.4.14 REQUISITOS PARA VERIFICAÇÃO DE OUTRAS FORMAS DE DIVULGAÇÃO DE REVOGAÇÃO

Não se aplica.

4.4.15 REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE

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

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

4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1 TIPOS DE EVENTO REGISTRADOS

4.5.1.1 EVENTOS OBRIGATÓRIOS RELACIONADOS AO SISTEMA DE CERTIFICAÇÃO QUE DEVERÃO SER INCLUIDOS EM ARQUIVOS DE AUDITORIA

a) Iniciação e desligamento do sistema de certificação;

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

c) Mudanças na configuração da AC Safeweb 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 Safeweb RFB ou de usuários finais;

h) Emissão e revogação de certificados;

i) Geração de LCR;

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

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

l) Operações de escrita nesse repositório, quando aplicável.

4.5.1.2 EVENTOS NÃO DIRETAMENTE RELACIONADOS AO SISTEMA DE CERTIFICAÇÃO

A AC Safeweb RFB registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

a) Registros de acessos físicos;

b) Manutenção e mudanças na configuração de seus sistemas;

c) Mudanças de pessoal e de perfis qualificados;

d) Relatórios de discrepância e comprometimento; e

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

4.5.1.3 A AC Safeweb RFB não registra outras informações.

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

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

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

a) Os agentes de registro que realizaram as operações;

b) Data e hora das operações;

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

d) A assinatura digital do executante.

4.5.1.7 A AC Safeweb RFB define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

4.5.2 FREQUÊNCIA DE AUDITORIA DE REGISTROS (*LOGS*)

AC Safeweb RFB examina os registros de auditoria uma vez por semana. Todos os eventos significativos são analisados e explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de 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 Safeweb RFB mantém localmente seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena os seus registros de auditoria da maneira descrita no item 4.6.

4.5.4 PROTEÇÃO DE REGISTRO (*LOGS*) DE AUDITORIA

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

4.5.4.2 Mecanismos de proteção utilizados:

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

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

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

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

4.5.5 PROCEDIMENTO PARA CÓPIA DE SEGURANÇA (*BACKUP*) DE REGISTRO (*LOG*) DE AUDITORIA

A AC Safeweb RFB gera a cada semana cópia de *backup* de seus registros de auditoria, através de procedimentos utilizando conexão segura.

4.5.6 SISTEMA DE COLETA DE DADOS DE AUDITORIA

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

4.5.7 NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC Safeweb RFB, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8 AVALIAÇÕES DE VULNERABILIDADE

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

4.6 ARQUIVAMENTO DE REGISTRO

4.6.1 TIPOS DE EVENTOS REGISTRADOS

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

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC Safeweb 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 evento arquivado, são:

a) As LCRs e os certificados de assinatura digital são retidos 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; e

c) As demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 6 (seis) anos.

4.6.3 PROTEÇÃO DE ARQUIVO

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

4.6.4 PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (*BACKUP*) DE ARQUIVO

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

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

4.6.5 REQUISITOS PARA DATAÇÃO DE REGISTROS (*TIME-STAMPING*)

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

4.6.6 SISTEMA DE COLETA DE DADOS DE ARQUIVO

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Safeweb RFB em seus procedimentos operacionais são automatizados, manuais e internos.

4.6.7 PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO

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

4.7 TROCA DE CHAVE

4.7.1 Trinta dias antes da data de expiração do certificado digital, a AR Vinculada comunica ao seu titular, através do e-mail cadastrado no formulário de solicitação de certificado, a data de expiração do certificado, junto com *link* para a solicitação de novo certificado.

4.7.2 Não se aplica.

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

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

O plano estabelecido conforme a PS da ICP-Brasil governa as situações de crise através da:

I – Identificação do motivo da crise;

II – Identificação dos responsáveis pelo processo de certificação digital;

III – Ativação das equipes envolvidas na solução do imprevisto;

IV – Definição da ação para impedir a continuidade do problema;

V – Avaliação da expansão da crise;

VI – Identificação das ações de recuperação propriamente ditas;

VII – Notificações à AC Raiz da evolução corretiva e solução, registro da crise e análise para melhoria.

4.8.1 RECURSOS COMPUTACIONAIS, SOFTWARE E DADOS CORROMPIDOS

4.8.1.1 Os procedimentos de recuperação utilizados pela AC responsável quando recursos computacionais, softwares ou dados estiverem corrompidos ou houver suspeita de corrupção, incluem, mas não se limitam a somente estes: a identificação da crise, acionamento dos principais gestores, ativação das equipes, contenção da crise, estimativa do alargamento da crise, declaração do início das atividades de ativação da situação de recuperação, notificação da crise, registro da crise, crítica para melhoria.

4.8.1.2 Nas circunstâncias de crise relacionadas aos recursos computacionais, softwares e dados corrompidos ou quando houver suspeita de corrupção desses componentes, após a identificação da crise ou confirmação da suspeita de corrupção, são comunicados os gestores de certificação digital, que acionam as equipes, de forma a identificar o grau de corrupção.

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

4.8.2 CERTIFICADO DE ENTIDADE É REVOGADO

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

4.8.3 CHAVE DE ENTIDADE É COMPROMETIDA

4.8.3.1 Em caso de comprometimento da chave da AC Safeweb RFB, após a identificação da crise são notificados os gestores do processo de certificação digital, que ativam as equipes envolvidas, de forma a indisponibilizar provisoriamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC Safeweb RFB e dos usuários finais, é gerado um novo par de chaves, emitido pela AC RFB certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para os usuários finais.

4.8.4 SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA NATUREZA

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

4.8.5 ATIVIDADES DAS AUTORIDADES DE REGISTRO

4.8.5.1 Procedimentos descritos no Plano de Continuidade do Negócio da(s) AR(s) Vinculada(s) contemplam a recuperação, total ou parcial das atividades das ARs, contendo, no mínimo as seguintes informações:

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

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 DE AC, AR ou PSS

4.9.1 Em caso de extinção da AC Safeweb RFB, AR Vinculada ou PSS serão adotadas os procedimentos previstos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

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

a) Notificar a AC Raiz da ICP-Brasil;

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

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

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

e) Preservar qualquer registro não transferido a um sucessor;

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

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

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

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

5.1 CONTROLES FÍSICOS

Nos itens seguintes estão descritos os controles físicos referentes às instalações que abrigam os sistemas da AC Safeweb RFB.

5.1.1 CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES DE AC

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

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

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

b) Instalações para sistemas de telecomunicações;

c) Sistemas de aterramento e de proteção contra descargas atmosféricas;

d) Iluminação de emergência.

5.1.2 ACESSO FÍSICO NAS INSTALAÇÕES DA AC SAFEWEB RFB

A AC Safeweb RFB inseriu um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a Política de Segurança implementada.

5.1.2.1 NÍVEIS DE ACESSO

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

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

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

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

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

5.1.2.1.6 No terceiro nível 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: senha individual e identificação biométrica.

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

5.1.2.1.8 No quarto nível – ou nível 4, interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Safeweb 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 no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9 No quarto nível todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. No quarto nível, 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 possuem proteção contra interferência eletromagnética externa.

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

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

a) Equipamentos de produção on-line;

b) Equipamentos de produção off-line e cofre de armazenamento.

5.1.2.1.12 O quinto nível – ou nível 5, interior aos ambientes de nível 4, compreende um cofre ou gabinete reforçado trancado. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

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

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

b) Possui tranca com chave e segredo.

5.1.2.1.14 O sexto nível – ou nível 6, consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de uma fechadura comum, com duas cópias de chave. Os dados de ativação da chave privada da AC SAFEWEB RFB são armazenados nesses depósitos.

5.1.2.2 SISTEMAS FÍSICOS DE DETECÇÃO

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

5.1.2.2.2 Os arquivos de imagens ou as fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Essas gravações são testadas (verificação de trechos aleatórios no início, meio e final do arquivo) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, um arquivo referente a cada semana. Essas gravações são armazenadas em ambiente de terceiro nível.

5.1.2.2.3 Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. Onde há, a partir do nível 2, vidros separando níveis de acesso foi implantado um mecanismo de alarme de quebra de vidros, que permanece ligado ininterruptamente.

5.1.2.2.4 Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não é satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais empregados, o critério mínimo de ocupação deixa de ser satisfeito, ocorre a reativação automática dos sensores de presença.

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

5.1.2.2.6 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 MECANISMO DE EMERGÊNCIA

5.1.2.4.1 Mecanismos específicos foram implantados pela AC Safeweb RFB para garantir a segurança de seu pessoal e de seus equipamentos 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 são documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.3 ENERGIA E AR CONDICIONADO NAS INSTALAÇÕES DE AC

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

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

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

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

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

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

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

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

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

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

a) Geradores de porte compatível;

b) Geradores de reserva;

c) Sistemas de nobreaks redundantes;

d) Sistemas redundantes de ar condicionado.

5.1.4 EXPOSIÇÃO À ÁGUA NAS INSTALAÇÕES DE AC

O ambiente de nível 4 encontra-se fisicamente protegido contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5 PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO NAS INSTALAÇÕES DE AC

5.1.5.1 Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas

que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

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

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

5.1.6 ARMAZENAMENTO DE MÍDIA NAS INSTALAÇÕES DE AC

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

5.1.7 DESTRUIÇÃO DE LIXO NAS INSTALAÇÕES DE AC

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

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

5.1.8 INSTALAÇÕES DE SEGURANÇA (*BACKUP*) EXTERNAS (*OFF-SITE*) PARA AC

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

5.1.9 INSTALAÇÕES TÉCNICAS DE AR

5.1.9.1 As instalações técnicas da(s) AR(s) Vinculada(s) atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

5.2 CONTROLES PROCEDIMENTAIS

5.2.1 PERFIS QUALIFICADOS

5.2.1.1 A AC Safeweb RFB efetua separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize o seu sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2 A AC Safeweb RFB estabelece perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. O detalhamento dos perfis encontra-se em documento interno normativo.

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

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

5.2.2 NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

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

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

5.2.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

5.2.3.1 Todo empregado da AC Safeweb RFB tem sua identidade e perfil verificados antes de:

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

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

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

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

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

a) São diretamente atribuídos a um único empregado;

b) Não são compartilhados;

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

5.3 CONTROLES DE PESSOAL

5.2.3.3 A AC Safeweb RFB implementa um padrão de utilização de "senhas fortes", definido na Política de Segurança implementada e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas. Todos os empregados da AC Safeweb RFB e da(s) AR(s) Vinculada(s) encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

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

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

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

5.3.1 ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE

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

5.3.2 PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

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

a) Verificação de antecedentes criminais;

b) Verificação de situação de crédito;

c) Verificação de histórico de empregos anteriores;

d) Comprovação de escolaridade e de residência.

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

5.3.3 REQUISITOS DE TREINAMENTO

Todo o pessoal da AC Safeweb RFB e da(s) AR(s) Vinculada(s) envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e mecanismos de segurança da AC Safeweb RFB e das AR vinculadas;

b) Sistema de certificação em uso na AC Safeweb 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 3.1.11; e

e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA

Todo o pessoal da AC Safeweb RFB e da(s) AR(s) Vinculada(s) envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC Safeweb RFB e da(s) AR(s) Vinculada(s).

5.3.5 FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

A AC Safeweb RFB e a AR Vinculada possuem pessoal e efetivo de contingência devidamente treinado, não fazendo uso de rodízio de pessoal.

5.3.6 SANÇÕES PARA AÇÕES NÃO AUTORIZADAS

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Safeweb RFB e da(s) AR(s) Vinculada(s), a AC Safeweb RFB ou a AR Vinculada suspenderá o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2 O processo administrativo referido acima contém os seguintes itens:

a) Relato da ocorrência com "*modus operandis*";

b) Identificação dos envolvidos;

c) Eventuais prejuízos causados;

d) Punições aplicadas, se for o caso; e

e) Conclusões.

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

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

a) Advertência;

b) Suspensão por prazo determinado; ou

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

5.3.7 REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

Todo o pessoal da AC Safeweb RFB e da(s) AR(s) Vinculada(s) envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e na Política de Segurança implementada pela AC Safeweb RFB.

5.3.8 DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.3.8.1 A AC Safeweb RFB torna disponível para todo o seu pessoal e para o pessoal da(s) AR(s) Vinculada(s):

a) Sua DPC AC Safeweb RFB;

b) As PCs que implementa;

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

d) Documentação operacional relativa a suas atividades;

e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2 Toda a documentação fornecida ao pessoal é classificada segundo a política de classificação de informação definida pela AC Safeweb RFB e é mantida atualizada.

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1 O par de chaves criptográficos da AC Safeweb RFB é gerado pela própria AC Safeweb RFB, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2 Pares de chaves são gerados somente pelo titular do certificado correspondente.

6.1.1.3 A geração do par de chaves de AC Safeweb RFB é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC Safeweb RFB, treinados para a função.

6.1.1.4 A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

6.1.1.5 O par de chaves da AC Safeweb RFB é gerado em módulo criptográfico de hardware no padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2 e V5) e no padrão obrigatório Homologação da ICP-Brasil NSH-2 ou NSH-3, conforme definido no DOC-ICP-01.01.

6.1.1.6 Somente os titulares dos certificados emitidos pela AC Safeweb RFB geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC Safeweb RFB.

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

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR

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

6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

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

6.1.3.2 Os procedimentos para a entrega da chave pública de um solicitante de certificado à AC Safeweb RFB estão detalhados em cada PC implementada.

6.1.4 DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC SAFEWEB RFB PARA USUÁRIOS

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

a) Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;

b) Diretório;

c) Página Web da AC Safeweb RFB www.safeweb.com.br;

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

6.1.5 TAMANHOS DE CHAVE

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

6.1.5.2 Não se aplica.

6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS

Os parâmetros de geração de chaves assimétricas da AC Safeweb RFB adotam o padrão *Federal Information Processing Standard* – FIPS 140-2, nível 3 (para as cadeias de certificação V2 e V5) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 ou NSH-3), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7 VERIFICAÇÃO DE QUALIDADE DOS PARÂMETROS

Os parâmetros são verificados de acordo com as normas estabelecidas pelo 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 Safeweb RFB é feito por hardware criptográfico com padrão de segurança “Homologação da ICP-Brasil NSH-3”, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8.2 Cada PC implementada pela AC Safeweb RFB caracteriza o processo utilizado para a geração de chaves criptográficas privativa dos titulares de certificados, com base nos requisitos

aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.9 PROPÓSITO DE USO DE CHAVE (CONFORME O CAMPO "*KEY USAGE*" NA X.509 V3)

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

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

6.2 PROTEÇÃO DA CHAVE PRIVADA

A AC Safeweb RFB implementa uma combinação de controles físicos (item 5.1.2), lógicos e procedimentais (item 5.2), de forma a garantir a segurança de suas chaves privadas.

As chaves privadas da AC Safeweb RFB são armazenadas de forma cifrada nos mesmos componentes seguros de hardware utilizados para sua geração. O acesso a esses componentes é controlado por meio de chave criptográfica de ativação.

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

6.2.1 PADRÕES PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC Safeweb RFB adota o padrão Federal Information Processing Standards – FIPS, 140-2, nível 3 (para as cadeias de certificação V2 e V5) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 e 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 está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]. Cada PC implementada especifica os requisitos aplicáveis à geração de chaves criptográficas dos titulares de certificado.

6.2.2 CONTROLE "N de M" PARA CHAVE PRIVADA

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

6.2.2.2 A AC Safeweb RFB estabelece como exigência de controle múltiplo para a utilização das suas chaves privadas:

a) Número mínimo de 2 ("n") (duas) pessoas de um grupo de 8 ("m") (oito) pessoas para utilização das suas chaves privadas.

6.2.3 RECUPERAÇÃO (*ESCROW*) DE CHAVE PRIVADA

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

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

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

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

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 A AC Safeweb RFB não emite certificados de sigilo. Não são arquivadas chaves privadas de assinatura digital.

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

Cada PC implementada define, quando aplicável, os requisitos para inserção da chave privada dos titulares de certificado em módulo criptográfico.

6.2.7 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

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

A confirmação da identidade desses detentores é feita através de crachás e senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Todos os eventos seguem cerimônias específicas. Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

6.2.8 MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

Para a desativação das chaves privadas da AC Safeweb RFB exige-se o número mínimo de 2 ("n") (dois) detentores de chaves criptográficas de um grupo de 8 ("m") (oito), conforme perfil qualificado. A confirmação da identidade desses detentores é feita através de crachás e senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Todos os eventos seguem cerimônias específicas. Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.9 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

Para a destruição das chaves privadas da AC Safeweb RFB exige-se o número mínimo de 2 ("n") (dois) detentores de chaves criptográficas de um grupo de 8 ("m") (oito), conforme perfil qualificado. A confirmação da identidade desses detentores é feita através de crachás e senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. As mídias de armazenamento das chaves privadas são reinicializadas de forma a não restarem nelas informações sensíveis. Cada PC implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

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

6.3.2 PERÍODOS DE USO PARA CHAVES PÚBLICAS E PRIVADAS

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

6.3.2.2 Não se aplica.

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

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

6.4 DADOS DE ATIVAÇÃO

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

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

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

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

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

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

6.4.3 OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO

Não se aplica.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

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

6.5.1.2 Os requisitos específicos aplicáveis são descritos em cada PC implementada.

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

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

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

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

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

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

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

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

6.5.2 CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL

A AC Safeweb RFB aplica configurações de segurança computacional baseadas no *Common Criteria* e desenvolvidas para o sistema operacional **Windows Server 2012 R2**. O fabricante

disponibiliza as atualizações do sistema operacional utilizado nos servidores do Sistema de certificação Digital da AC Safeweb RFB.

6.5.3 CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO

6.5.3.1 A AC Safeweb RFB implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela AR Vinculada para os processos de validação e aprovação de certificados.

6.5.3.2 São incluídos os seguintes requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

As estações de trabalho da AR, incluindo equipamentos portáteis, estão protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos e recebem as seguintes configurações de segurança:

a) Controle de acesso lógico ao sistema operacional;

b) Exigência de uso de senhas fortes;

c) Diretivas de senha e de bloqueio de conta;

d) *Logs* de auditoria do sistema operacional ativados, registrando:

I – Iniciação e desligamento do sistema;

II – Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;

III – Mudanças na configuração da estação;

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

V – Tentativas não-autorizadas de acesso aos arquivos de sistema;

VI – Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.

e) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;

f) *Firewall* pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por *firewall* corporativo, para equipamentos instalados em redes que possuam esse dispositivo;

g) Proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;

h) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.);

i) Utilização apenas de *softwares* licenciados e necessários para a realização das atividades do usuário;

j) Impedimento de *login* remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;

k) Utilização da data e Hora Legal Brasileira.

Os *logs* de auditoria do sistema operacional registram os acessos aos equipamentos e ficam armazenados localmente por um período mínimo de 60 dias.

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

O Agente de Registro não possui perfil de administrador ou senha de *root* dos equipamentos, ficando essa tarefa delegada a terceiros da própria organização, para permitir segregação de funções.

O aplicativo que faz interface entre a AR e o sistema de certificação da AC possui as seguintes características de segurança:

a) Acesso permitido somente mediante autenticação por meio do certificado do tipo A3 de Agente de Registro, devidamente habilitado no sistema da AC;

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

c) *Timeout* de sessão de acordo com a análise de risco da AC;

d) Registro em *log* de auditoria dos eventos citados no item 4.5.1 do DOC-ICP-05 [1];

e) Histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas;

f) Registro em *log*, para em cada certificado emitido, informando se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da AR;

g) Mecanismo para revogação automática dos certificados digitais emitidos fora do ambiente da AR e que não tenham sido verificados pelo segundo Agente de Registro, mediante cópia da documentação apresentada na etapa de validação, até o momento do início da validade do certificado.

O aplicativo da AR:

a) Foi desenvolvido com documentação formal;

b) Possui mecanismos para controle de versões;

c) Possui documentação dos testes realizados em cada versão;

d) Possui documentação comprovando a homologação de cada versão em ambiente com as mesmas características do que será usado em produção, sendo esses ambientes, porém, obrigatoriamente apartados entre si;

e) Possui aprovação documentada do gerente da AC, ou responsável designado, para colocar cada versão em ambiente de produção.

Os *logs* gerados por esse aplicativo são armazenados na AC pelo prazo de 6 (seis) anos, conforme previsto no item 4.6.2. do DOC-ICP-05.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.6.1.1 A AC Safeweb RFB adota tecnologias de certificação digital e efetua as devidas customizações para adequar as necessidades do ambiente da AC, as quais são desenvolvidas por empregados da AC Safeweb RFB. Essas customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluídas são colocadas em um ambiente de homologação. Finalizado o processo de homologação é encaminhado um pedido para o Gerente da AC, que avalia e decide quanto à sua implementação.

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

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.6.2.1 A AC Safeweb RFB e ARs vinculadas utilizam ferramentas e os procedimentos formais para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

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

6.6.3 CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA

Não se aplica.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

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

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 DIRETRIZES GERAIS

6.7.1.1 Neste item são descritos os controles relativos à segurança da rede da AC Safeweb RFB, incluindo *firewalls* e recursos similares.

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

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

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

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

6.7.2 *FIREWALL*

6.7.2.1 Mecanismos de *firewall* são implementados em equipamentos de utilização específica configurados exclusivamente para tal função. *Firewalls* promovem o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo, a conhecida "zona desmilitarizada" (DMZ) - em relação aos equipamentos com acesso exclusivamente interno à AC Safeweb 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 ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps*

SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta aos *firewalls* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração dos *firewalls*.

6.7.3.2 O sistema de detecção de intrusão 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 - são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é, no mínimo, diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

6.8.1 O módulo criptográfico utilizado para armazenamento da chave privada da AC Safeweb RFB adota o padrão *Federal Information Processing Stardards* – FIPS, 140-2, nível 3 (para as cadeias de certificação V2 e V5) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 e NSH-3), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.8.2 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 itens seguintes, são descritos os aspectos dos certificados e LCR emitidas pela AC Safeweb RFB.

7.1.2 As PCs abaixo, implementadas pela AC Safeweb RFB, especificam os formatos dos certificados gerados e das correspondentes LCRs. Nessas PCs são incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

POLÍTICA DE CERTIFICADO	NOME CONHECIDO	OID
Política de Certificado de Assinatura Digital tipo A1 da AC Safeweb RFB	PC AC Safeweb RFB A1	2.16.76.1.2.1.51
Política de Certificado de Assinatura Digital tipo A3 da AC Safeweb RFB	PC AC Safeweb RFB A3	2.16.76.1.2.3.48

7.1.3 Não se aplica.

7.2 PERFIL DO CERTIFICADO

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

7.2.2 EXTENSÕES DE CERTIFICADO

Não se aplica.

7.2.3 IDENTIFICADORES DE ALGORITMO

Não se aplica.

7.2.4 FORMATOS DE NOME

Não se aplica.

7.2.5 RESTRIÇÕES DE NOME

Não se aplica.

7.2.6 OID (*OBJECT IDENTIFIER*) DE DPC

O OID desta DPC AC Safeweb RFB é 2.16.76.1.1.64.

7.2.7 USO DA EXTENSÃO "*POLICY CONSTRAINTS*"

Não se aplica.

7.2.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Não se aplica.

7.2.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS

Não se aplica.

7.3 PERFIL DE LCR

7.3.1 NÚMERO(s) DE VERSÃO

As LCRs geradas pela AC Safeweb 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 Neste item são descritas todas as extensões de LCR utilizadas pela AC Safeweb RFB e sua criticidade.

7.3.2.2 As LCRs da AC Safeweb RFB obedecem a ICP-Brasil que define como obrigatórias as seguintes extensões:

a) "*Authority Key Identifier*", não crítica: contém o hash SHA-1 da chave pública da AC que assina a

LCR;

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

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração nesta DPC AC Safeweb RFB é submetida à aprovação do CG da ICP-Brasil. Esta DPC - AC Safeweb RFB é atualizada sempre que uma nova PC implementada pela AC Safeweb RFB o exigir.

8.2 POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

Esta DPC - AC Safeweb RFB está disponível para a comunidade no endereço web: www.safeweb.com.br.

8.3 PROCEDIMENTOS DE APROVAÇÃO

Esta DPC - AC Safeweb RFB foi submetida à aprovação, durante o processo de credenciamento da AC Safeweb RFB, bem como suas atualizações, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9 DOCUMENTOS REFERENCIADOS

9.1 RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-Brasil

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

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES	DOC-ICP-09

	INTEGRANTES DA ICP-BRASIL	
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

9.2 INSTRUÇÕES NORMATIVAS DA AC RAIZ

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
[1]	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
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	DOC-ICP-05.02
[11]	REGULAMENTO DO USO DE BIOMETRIA NO ÂMBITO DA ICP-BRASIL – SISTEMA BIOMÉTRICO DA ICP-BRASIL	DOC-ICP-05.03
[12]	REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS	DOC-ICP-01.02

9.3 DOCUMENTOS DA AC RAIZ

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

10 LISTA DE ACRÔNIMOS

AC Autoridade Certificadora
AC Raiz Autoridade Certificadora Raiz da ICP-Brasil

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	Infra-Estrutura 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	*Online 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*
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SNMP	*Simple Network Management Protocol*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação
URL	*Uniform Resource Location*