Declaração de Práticas de Certificação
DPC

Autoridade Certificadora VALID

para a Secretaria da Receita Federal do Brasil

DPC da AC VALID RFB
Versão 5.0
Outubro de 2018

Sumário

Autor: *Valid Certificadora Digital Ltda.*
Edição: *Outubro de 2018*
Versão: *5.0*

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos mínimos, observados obrigatoriamente pela Autoridade Certificadora Valid para a Receita Federal do Brasil, AC integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução dos seus serviços.

1.1.2. Toda DPC elaborada no âmbito da ICP-Brasil adota obrigatoriamente a mesma estrutura empregada no documento "REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [5]". A Autoridade Certificadora Valid para a Receita Federal do Brasil (AC VALID RFB) está no nível imediatamente subsequente ao da Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB). As informações sobre a administração e geração dos tipos de certificados emitidos pela AC VALID RFB, são apresentados nas Políticas de Certificado (PCs) que podem ser consultadas no endereço eletrônico: http://www.validcertificadora.com.br/ac-valid-rfb

1.2. Identificação

Este documento denominado "Declaração de Práticas de Certificação" (DPC), comumente referido como "DPC AC VALID RFB" identifica procedimentos e práticas empregados no âmbito da ICP-Brasil. O OID (*Object Identifier*) atribuído à esta DPC é o 2.16.76.1.1.45.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridade Certificadora (AC)

Esta DPC refere-se unicamente à AC VALID RFB, (Avenida Paulista, nº 2064, 15º andar, São Paulo, SP, CEP: 01310-928 sob CPNJ 14.121.957/0001/09), no âmbito da ICP-Brasil, encontra se pulicada no seu repositório, no seguinte endereço: http://www.validcertificadora.com.br/Declaracao-de-Praticas-de-Certificacao/D379

1.3.2. Autoridade de Registro (AR)

1.3.2.1. No endereço eletrônico http://www.validcertificadora.com.br/ac-valid-rfb constam as Autoridades de Registro (ARs) vinculadas à AC VALID RFB, estas responsáveis nas competências dos processos de recebimento, validação e encaminhamento das solicitações de emissão e revogação dos certificados digitais e na identificação dos seis solicitantes. O endereço contém:

a) relação de todas as Ars credenciadas, com informações sobre as PCs que implementam;

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

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

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

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data 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 VALID RFB manterá as informações descritas acima sempre atualizadas.

1.3.3. Prestador de Serviços de Suporte

1.3.3.1. No endereço eletrônico http://www.validcertificadora.com.br/ac-valid-rfb constam os Prestadores de Serviço de Suporte – PSS, vinculados à AC VALID RFB.

1.3.3.2. PSS são entidades utilizadas pela AC VALID RFB ou pelas Ars vinculadas para desempenhar atividades descritas nesta DPC ou nas PCs 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.

1.3.3.3. A AC VALID RFB manterá as informações descritas acima sempre atualizadas.

1.3.3.A. Prestador de Serviços de Confiança

1.3.3.A.1 A relação de todos os Prestadores de Serviço de Confiança – PSC vinculados diretamente a AC VALID RFB é publicada em serviço de diretório e/ou em página web da AC VALID RFB (http://www.validcertificadora.com.br/ac-valid-rfb)

1.3.4. Titulares de Certificado

Podem ser titulares de certificados digitais emitidos pela AC VALID RFB, pessoas físicas inscritas no Cadastro de Pessoas Físicas – CPF, desde que não enquadradas na situação cadastral de CANCELADA, e pessoas jurídicas inscritas no Cadastro Nacional de Pessoas Jurídicas – CNPJ, desde que não enquadradas na condição de BAIXADA, INAPTA, SUSPENSA ou CANCELADA, conforme o disposto nos incisos I e II do art. 6º da Instrução Normativa RFB n 1077, de 29 de Outubro de 2010.
Sendo o titular do certificado de pessoa jurídica, será designada pessoa física como responsável pelo uso do certificado, que será o detentor da chave privada. Obrigatoriamente, o responsável pelo uso do certificado é o mesmo responsável pela pessoa jurídica cadastrado na RFB.
Em se tratando de certificado digital emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

1.3.5. Aplicabilidade

A AC VALID RFB implementa as seguintes Políticas de Certificado:

POLÍTICA DE CERTIFICADO	NOME	OID
Política de Certificado de Assinatura Digital do tipo A1 da AC VALID RFB	PC A1 da AC VALID RFB	2.16.76.1.2.1.37

Política de Certificado de Assinatura Digital do tipo A3 da AC VALID RFB	PC A3 da AC VALID RFB	2.16.76.1.2.3.36

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

1.4. Dados de Contato

Empresa: Valid Certificadora Digital Ltda.
Endereço: Avenida Paulista, nº 2064, 15º Andar, São Paulo, SP
CEP: 03310-928
Página da Web: http://www.validcertificadora.com.br/

Área: Normas e *Compliance*
Telefones: +55 11 2575-6800
Mail: pki.compliance@valid.com

2. DISPOSIÇÕES GERAIS

2.1. Obrigações e direitos

2.1.1 Obrigações da AC VALID RFB

As obrigações são as abaixo relacionadas:

a) operar de acordo com a esta DPC AC VALID RFB e com as PCs que implementa;

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

c) assegurar a proteção de suas chaves privadas;

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

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

f) distribuir o seu próprio certificado;

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

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta online de situação do certificado (OCSP – *On-line Certificate Status Protocol*);

k) publicar em sua página web sua DPC AC VALID RFB e as PCs aprovadas que implementa no endereço: http://www.validcertificadora.com.br/Declaracao-de-Praticas-de-Certificacao/D379;

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

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

n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;

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

p) adotar as medidas de segurança e controle previstas na DPC AC VALID RFB, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

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

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

s) manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;

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

v) informar à AC Raiz, 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.

2.1.2. Obrigações das Ars

As obrigações das Ars vinculadas à AC VALID RFB são as abaixo relacionadas:

a) receber solicitações de emissão ou de revogação de certificados;

b) confirmar a identidade do solicitante e a validade da solicitação;

c) encaminhar a solicitação de emissão ou de revogação de certificado à AC VALID RFB utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1];

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

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

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

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

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

São as obrigações do titular de certificado digital emitido pela AC VALID RFB, constantes dos termos de titularidade de que trata o item 4.1.1, são as abaixo relacionadas:

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

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

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

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

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

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

2.1.4. Direitos da Terceira Parte (*Relying Party*)

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

2.1.4.2. Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos na DPC ou 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 VALID RFB e do titular do certificado.

2.1.5. Obrigações do Repositório

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

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

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

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

2.2 Responsabilidades

2.2.1. Responsabilidades da AC VALID RFB

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

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

2.2.1.3. Não se aplica.

2.2.1.4. Não se aplica.

2.2.2 Responsabilidade da AR

As Ars vinculadas à AC VALID RFB serão responsáveis pelos danos a que derem 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 VALID RFB e ARs a ela vinculadas, exceto na hipótese de prática de ato ilícito. Nesse caso, a terceira parte deverá indenizar a AC VALID 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 VALID RFB dispõe de uma apólice de seguro de responsabilidade civil que se estende a todos os titulares de certificados digitais por ela emitidos.

A AC VALID RFB ou suas ARs vinculadas, indenizarão integralmente os danos a que comprovadamente derem causa, limitados ao valor máximo coberto pela apólice, caso o cliente seja Pessoa Jurídica.
A apólice de seguro de responsabilidade civil cobre perdas e danos decorrentes de comprometimento da chave privada da AC VALID RFB, de erro na identificação do titular, de emissão defeituosa do certificado ou de erros ou omissões da AC VALID RFB e das ARs vinculadas na prestação de seus serviços.

2.3.3. Processos Administrativos

O titular do certificado que sofrer perdas e danos decorrentes do uso do certificado digital emitido pela AC VALID RFB tem o direito de comunicar à AC VALID RFB que deseja a indenização prevista no item 2.3.2 acima, observadas as seguintes condições:

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC VALID RFB, tal comprometimento deverá ter sido comprovado por perícia realizada por perito especializado e independente;

b) nos casos de erro na identificação, o titular do certificado não pode requerer qualquer indenização quando os dados constantes no certificado corresponderem aos dados fornecidos por esse titular à AC VALID RFB ou às ARs vinculadas;

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

2.4. Interpretação e Execução

2.4.1. Legislação

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

2.4.2. Forma de interpretação e notificação

2.4.2.1. Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, o corpo técnico da AC VALID RFB examinará a disposição inválida e irá propor, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada. As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.2.2. Todas solicitações, notificações ou quaisquer outras comunicações necessárias, relativas às práticas descritas na DPC, realizadas por iniciativa da AC VALID RFB, serão enviadas por e-mail assinado pelos responsáveis pela AC.

2.4.3. Procedimentos de solução de disputa

2.4.3.1. Esta DPC prevalece sobre quaisquer outros documentos como planos, declarações, políticas, acordos e contratos que a AC VALID RFB venha a adotar. Pode haver documentos complementares ou normativos, os quais não podem contrariar esta DPC. Em caso de conflito o documento conflitante deve ser ignorado ou alterado.

2.4.3.2. Em caso de conflito entre esta DPC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nessa situação está DPC será alterada para a solução da disputa.

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

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e renovação de certificados

A AC VALID RFB define tarifas para emissão ou renovação de certificados conforme estabelecido em sua página web: http://www.validcertificadora.com.br ou em contrato comercial específico.

2.5.2. Tarifas de acesso ao certificado

Não há tarifas previstas pela AC VALID RFB para o acesso a seu certificado.

2.5.3. Tarifas de revogação ou de acesso à informação de status

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

2.5.4. Tarifas para outros serviços, tais como informação de política

Não há tarifas previstas pela AC VALID RFB para outros serviços.

2.5.5. Política de reembolso

Caso o certificado do titular deva ser revogado por motivo de comprometimento da chave privada da AC VALID RFB ou da mídia armazenadora da chave privada da AC VALID RFB, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC VALID RFB, será emitido outro certificado em substituição, sem cobrança.

2.6. Publicação e Repositório

2.6.1. Publicação de informação da AC VALID RFB

2.6.1.1. A AC VALID RFB publica e disponibiliza informações, tais como certificados, LCR, sua DPC, entre outras, com disponibilidade de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As informações abaixo são publicadas na página web da AC VALID RFB no endereço http://www.validcertificadora.com.br/ac-valid-rfb :

a) seu próprio certificado;

b) suas LCRs;

c) esta DPC;

d) as PCs que implementa;

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

A AC VALID RFB manterá as informações de que trata o item anterior sempre atualizadas.

2.6.3. Controles de acesso

Não há qualquer restrição ao acesso para consulta às informações citadas no item 2.6.1. Acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis, designadas especificamente para esse fim. Os controles de acesso incluirão identificação pessoal para acesso aos equipamentos, utilização de senhas e utilização de protocolos seguros de comunicação de dados.

2.6.4. Repositórios

O repositório da AC VALID RFB está disponível para consulta e atende aos seguintes requisitos:

a) endereço: http://www.validcertificadora.com.br/ac-valid-rfb
b) disponibilidade: aquela definida no item 2.6.1 desta DPC AC VALID RFB;
c) protocolo de acesso: HTTP;
d) características de segurança: aquelas definidas no item 5 desta DPC AC VALID RFB.

2.6.4.1. A AC VALID RFB disponibiliza 02 (dois) repositórios, em infraestrutura de rede segregadas, para distribuição de LCR. São eles:

http://www.receita.fazenda.gov.br/acrfb/acrfbv3.crl

http://www.receita.fazenda.gov.br/acrfb/acrfbv4.crl

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 e com os princípios e critérios definidos pelo *WebTrust*.

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 CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de

seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

2.7.4. A AC VALID 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. As entidades da ICP-Brasil diretamente vinculadas à AC VALID RFB também receberam auditoria prévia, para fins de credenciamento. A AC VALID RFB é 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. As chaves privadas de assinatura digital da AC VALID RFB, responsável pela DPC, são geradas e mantidas pela própria AC VALID RFB, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC VALID RFB é de sua inteira responsabilidade.

2.8.1.2. Os titulares de certificados emitidos pela AC VALID RFB, ou os responsáveis pelo seu uso, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além disso, são responsáveis pela divulgação ou utilização dessas 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 VALID 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 VALID RFB ou às ARs vinculadas deverá ser divulgado.

2.8.3. Tipos de informações não sigilosas

2.8.3.1. Não são consideradas informações sigilosas pela AC VALID RFB e ARs vinculadas:

a) os certificados e as LCRs emitidos pela AC VALID RFB;

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

c) as PCs implementadas pela AC VALID FRB;

d) a DPC da AC VALID RFB;

e) versões públicas de Políticas de Segurança; e

f) a conclusão dos relatórios de auditoria.

2.8.3.2. A AC VALID RFB e as ARs vinculadas tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) estejam na posse legítima da AC VALID RFB e das ARs vinculadas antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;

b) posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação, sem quaisquer restrições para tal;

c) sejam requisitados por determinação judicial ou governamental, desde que a AC VALID RFB e as ARs vinculadas comuniquem previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

2.8.3.3. Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC VALID RFB e as ARs vinculadas, exceto na hipótese da alínea 'c' acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

2.8.4. Divulgação de informação de revogação ou suspensão de certificado

2.8.4.1. A AC VALID RFB disponibiliza a lista de certificados revogados em seu repositório, http://www.validcertificadora.com.br/ac-valid-rfb . Os motivos que justificaram a revogação são mantidos confidenciais pela AC VALID RFB e pelas ARs vinculadas, exceto quando:

a) o titular do certificado revogado autorizar expressamente a sua divulgação a terceiros;

b) esses motivos tenham sido publicados ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da AC VALID RFB ou das ARs vinculadas;

c) tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC VALID RFB ou ARs vinculadas, se estiver obrigada a responde-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

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

2.8.5. Quebra de sigilo por motivos legais

A AC VALID RFB tem o dever de fornecer documentos, informações ou registro sob sua guarda, mediante ordem judicial.

2.8.6. Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC VALID 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. O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

2.8.7.2. Nenhuma liberação de informação é permitida sem autorização formal do titular do certificado, exceto nos casos previstos no item 2.8.5. Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou
b) por meio de pedido escrito com firma reconhecida.

2.8.8. Outras circunstâncias de divulgação de informação

Em nenhuma outra circunstância, que não esteja prevista nesta DPC, serão divulgadas informações sigilosas.

2.9. Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual inclusive os direitos autorais em todos os certificados e todos os documentos gerados para a AC VALID RFB (eletrônicos ou não), pertencem e continuarão sendo de propriedade da AC VALID RFB. Direitos sobre Identificadores de Objeto (OID) atribuídos à AC VALID RFB após o processo de credenciamento cabem única e
exclusivamente à AC Raiz da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Registro Inicial

3.1.1. Disposições Gerais

3.1.1.1. As Autoridades de Registro – ARs vinculadas à AC VALID RFB, utilizarão os seguintes requisitos e procedimentos para a realização dos procedimentos que seguem:

9) 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, 3.1.10 e 3.1.11:

9. <u>confirmação da identidade de um indivíduo:</u> 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 de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC VALID RFB;

b) Verificação da solicitação de certificado – 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 dos 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. Excepcionalmente, o processo de validação poderá ser realizado fora do ambiente físico da AR, através de procedimento de validação externa, mediante o deslocamento do Agente de Registro da AR até o interessado na obtenção do certificado, observadas as hipóteses, a forma e as condições abaixo dispostas, vedada a criação de instalações físicas destinadas a tal fim, qualquer que seja a denominação utilizada, tais como, mas não limitada a ponto de atendimento, posto de validação, parceiro, canal, agente credenciado ou agência autorizada.

3.1.1.2.1. As ARs poderão adotar o procedimento de validação externa nas seguintes hipóteses:

I. Para pessoas com deficiência ou com mobilidade reduzida, conforme definido pela Lei nº 13.146, de 6 de julho de 2015, devidamente comprovado por documento hábil;

II. Para pessoas Politicamente Expostas – PEP, conforme definido na Resolução nº 16, de 28 de março de 2007, do Conselho de Controle de Atividades Financeiras COAF/MF, devidamente comprovado por documento hábil;

III. Para pessoas que se encontrem cumprindo pena ou detidas em estabelecimento prisional;

IV. Para pessoas com incapacidade física momentânea ou por motivo de saúde, em qualquer caso devidamente justificado e comprovado por documento hábil, estejam impedidas ou impossibilitadas de se deslocar até a instalação física da AR;

V. Para atender contratos firmados com entidades públicas cujos os editais de licitação tenham sido publicados até a data de publicação desta Resolução;

VI. Outras pessoas não citadas anteriormente, mediante solicitação expressa de validação externa pelo titular do certificado, limitado a 15% (quinze por cento) do total de certificados emitidos pela AR no mês imediatamente anterior.

Nota 1: O disposto na alínea VI, aplica-se a partir do mês subsequente à entrada em operação da AR, vedada a validação externa com base no referido dispositivo, no mês do início de sua operação.

Nota 2: Considera-se como total de certificados emitidos pela AR no mês imediatamente anterior, para fins da alínea VI, o volume de certificados emitidos pela AR, informado na documentação encaminhada ao ITI na forma e no prazo previsto pela Instrução Normativa no 14, de 28 de novembro de 2016.

Nota 3: Acaso a AR não tenha emitido certificados no mês anterior ou não tenham sido prestadas as informações na forma ou no prazo exigidos, ficará a AR impossibilitada de emitir novos certificados com fulcro na alínea VI, somente podendo voltar a emiti-los no mês imediatamente subsequente, desde que prestadas as informações de forma tempestiva.

Nota 4: Para o cálculo da quantidade limite disposto na alínea VI, em caso de resultado fracionário, admitir-se-á o arredondamento para a unidade superior.

3.1.1.2.2. A validação externa será realizada no domicílio do titular do certificado digital, nas hipóteses previstas nos incisos I, II e IV, do item 3.1.1.2.1, ou no local que este se encontre, na hipótese do inc. III, do mesmo item.

3.1.1.2.3. Para fins do item anterior, considera-se domicílio do titular do certificado digital, o seu domicílio civil, na forma do disposto no Código Civil, Lei nº 10.406, de 10 de janeiro de2002.

3.1.1.2.4. O local no qual a validação externa será realizada deverá ser informado no Formulário de Validação Externa, a que se refere a alínea 'd' do item 3.1.1.2.5.

3.1.1.2.5. A validação fora do ambiente físico da AR deve atender ainda as seguintes condições:

a) utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR;

b) adotar aplicativo de georreferenciamento que permita rastrear o computador móvel utilizado na validação externa, sendo que a localização do equipamento deve ficar disponível no sistema da AR em que o agente de registro deva estar cadastrado previamente;

c) adotar equipamentos de coleta e verificação biométrica do titular e do agente de registro, em atendimento aos padrões da ICP-Brasil;

d) preencher o Formulário de Validação Externa, adendo ADE-ICP-05.D (modelo disponibilizado em https://www.iti.gov.br/legislacao/adendos), o qual deverá ser assinado pelo agente de registro e pelo titular do certificado, preferencialmente assinados digitalmente;

e) em se tratando de dossiês físicos do titular de certificado, esses devem ser enviados para a Instalação Técnica em até 5 (cinco) dias úteis; e

f) Utilização de equipamento específico, destinado exclusivamente para fins de validação externa, vedada a utilização, para tal fim, das estações de trabalho ou outros equipamentos empregados na instalação técnica.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado devem ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC VALID 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 ARs 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 VALID RFB disponibiliza para todas as ARs vinculadas à sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

3.1.1.8. Não se aplica.

3.1.1.9. Não se aplica.

3.1.1.10. Não se aplica.

3.1.1.11. Não se aplica.

3.1.2. Tipos de nomes

3.1.2.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "*Distinguished Name*" do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular. O certificado emitido para pessoa jurídica inclui o nome da pessoa física responsável. Para todos os efeitos legais, os certificados e as respectivas chaves de assinatura são de titularidade do responsável constante do certificado.

3.1.2.2. Não se aplica.

3.1.3. Necessidade de nomes significativos

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

Para certificados de pessoa física, o campo *Common Name* é composto do nome do titular do certificado, conforme consta no Cadastro de Pessoa Física – CPF junto à RFB.
Para os certificados de pessoa jurídica o campo *Common Name* é composto do nome empresarial (Razão Social) da pessoa jurídica, conforme consta no Cadastro Nacional de Pessoa Jurídica – CNPJ, junto à RFB.

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Os identificadores "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado emitido pela AC VALID RFB. Números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo DN, conforme o padrão ITU X.509.

3.1.6. Procedimento para resolver disputa de nomes

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

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

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

3.1.8. 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 segundo o padrão definido na RFC 2510, item 2.3 – *Proof of Possession (POP) of Private Key*.

3.1.9. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos pessoais de identificação legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

Antes à solicitação do certificado, é realizada consulta da situação cadastral do solicitante, CPF e ou CNPJ, conforme incisos I e II do art. 6º da Instrução Normativa RFB N° 1077. Se os status se enquadrarem nas situações citadas, a solicitação não será enviada à AC VALID 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) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial; e

e) Mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4.

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

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

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

Nota 4: Não se aplica.

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

Nota 6: Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento 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: Não se aplica.

Nota 9: Os documentos que possuem data de validade precisam estar dentro do prazo, à exceção da CNH que permanece válida como documento de identificação mesmo que sua data de validade esteja expirada (Oficio Circular nº 2/2017/CONTRAN, de 29 de junho de 2017).

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) nome completo, sem abreviações;
b) data de nascimento;
c) não se aplica.

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) Cadastro de Pessoa Física (CPF);

b) número de Identificação Social – NIS (PIS, PASEP ou CI);

c) número do Registro Geral – RG do titular e órgão expedidor;

d) número do Cadastro Especifico do INSS (CEI);

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

f) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente;

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, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.10. Autenticação da identidade de uma organização

3.1.10.1.1. Os procedimentos para confirmação da identidade de uma organização são os definidos a seguir.

3.1.10.1.2. Será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

3.1.10.1.3. A confirmação da identidade da organização e das pessoas físicas é feita nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.1.10.2;

b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;

c) presença física dos representantes legais e do responsável pelo uso do certificado;

d) assinatura do termo de titularidade de que trata o item 4.1.1 pelo titular ou responsável pelo uso do certificado.

NOTA 01: A AC VALID RFB e ARs vinculadas podem solicitar assinatura manuscrita ao titular e/ou responsável pelo uso do certificado para comparação com o documento de identidade ou contrato social.

3.1.10.2. Documentos para efeitos de identificação de uma organização

A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos à sua habilitação jurídica:

i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;

ii. se entidade privada:

1. ato constitutivo, devidamente registrado no órgão competente; e
2. documentos da eleição de seus administradores, quando aplicável;

b) Relativos à sua habilitação fiscal:

i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou

ii. prova de inscrição no Cadastro Específico do INSS – CEI.

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 Pessoa Jurídica (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, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.1.9.2.

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Disposições Gerais

3.1.11.1.1. Em se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

3.1.11.1.2. Se o titular for pessoa física, deverá ser feita a confirmação de sua identidade na forma do item 3.1.9.1. e este assinará o termo de titularidade de que trata o item 4.1.1.

3.1.11.1.3. Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) Apresentação do rol de documentos elencados no item 3.1.10.2;

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

c) Presença física do responsável pelo uso do certificado e assinatura do termo de responsabilidade de que trata o item 4.1.1; e

d) Presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade de que trata o item 4.1.1, ou outorga de procuração atribuindo poderes para solicitação de certificado para equipamento ou aplicação e assinatura do respectivo termo de titularidade.

3.1.11.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.1.11.2.1. Para certificados de equipamento ou aplicação que utilizem URL no campo *Common Name*, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele nome. Nesse caso deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

3.1.11.2.2. Não se aplica.

3.1.11.3. Informações contidas no certificado emitido para um equipamento ou aplicação

3.1.11.3.1. É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nos documentos apresentados:

a) URL ou nome da aplicação;

b) nome completo do responsável pelo certificado, sem abreviações;

c) data de nascimento do responsável pelo certificado;

d) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o titular for pessoa jurídica;

e) Cadastro Nacional de Pessoa Jurídica (CNPJ), se o titular for pessoa jurídica.

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

3.1.12. Autenticação de identificação de equipamento para certificado CF-e-SAT

Esse item não se aplica.

3.1.13. Autenticação de identificação de equipamentos para certificado OM-BR

Esse item não se aplica.

3.2. Geração de novo par de chaves antes da expiração do atual

3.2.1. No item seguinte estão estabelecidos os processos de identificação do solicitante utilizados pela AC VALID 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 citado acima é conduzido segundo uma das seguintes possibilidades:

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

b) Em caso de pessoa jurídica, qualquer alteração em sua constituição e funcionamento deverá constar do processo de renovação.

c) 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 expiração ou revogação

3.3.1. Após a revogação ou expiração do certificado, os procedimentos utilizados para confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo descritos nas PCs implementadas.

3.3.2. Não se aplica.

3.4. Solicitação de Revogação

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas. O procedimento para solicitação de revogação de certificado emitido pela AC VALID RFB está descrito no item 4.4.3. desta DPC.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado

4.1.1. Para atender a solicitação de certificado digital à AC VALID RFB e suas ARs vinculadas, os requisitos e procedimentos deverão compreender, no mínimo:

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

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

c) um termo de titularidade assinado pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE

TITULARIDADE [4] específico, e, ainda, quando emissão para servidor público da ativa e militar da União pela autoridade designada formalmente pelos órgãos competentes.

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. A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento do "Termo de Titularidade", no caso de certificados de pessoas jurídicas, equipamentos ou aplicações e dos demais documentos exigidos. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e o titular é notificado por e-mail, sobre a emissão e do método para a retirada do certificado.

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

4.3. Aceitação de Certificado

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

a) concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;

b) garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa;

d) Torna-se responsável por todos os atos praticados perante a RFB utilizando a chave privada correspondente à chave pública contida no certificado.

4.3.2. A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado ou responsável pelo uso no caso de certificado para pessoa jurídica, na primeira utilização da chave privada correspondente.

4.3.3. Não se aplica.

4.4. Suspensão e Revogação de Certificado

4.4.1. Circunstâncias para revogação

4.4.1.1. Este item caracteriza circunstâncias nas quais o titular do certificado ou o responsável pelo uso do certificado pode solicitar a revogação de seu certificado, a qualquer tempo.

4.4.1.2. Um certificado é obrigatoriamente revogado:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;
b) Quando for necessária a alteração de qualquer informação constante no mesmo;
c) No caso de extinção, dissolução ou transformação da AC VALID RFB;
d) No caso de perda, roubo, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora;
e) por decisão judicial;
f) no caso de falecimento do titular – pessoas físicas;
g) no caso de extinção, dissolução ou transformação do titular do certificado – equipamentos, aplicações e pessoas jurídicas; ou
h) no caso de falecimento ou demissão do responsável – equipamentos, aplicações e pessoas jurídicas.

4.4.1.3. A DPC deve observar ainda que:

a) A AC VALID RFB deverá revogar, 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; e
b) O CG da ICP-Brasil ou a AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.4.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser solicitada:

a) Por solicitação do titular do certificado;
b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
d) Pela AC VALID RFB;
e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz;
g) Não se aplica;
h) Não se aplica;
i) Não se aplica;
j) Não se aplica;
k) Decisão judicial.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. A AC VALID RFB garante que todos os habilitados, conforme o item 4.4.2. Podem, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados. A solicitação de revogação é encaminhada à AC VALID RFB por meio de formulário on-line, disponibilizado na página web http://www.validcertificadora.com.br/revogue . Para tanto, o titular ou responsável pelo uso deve fornecer os dados do certificado (número do ticket ou CPF/CNPJ) e a senha de identificação, indicada na solicitação de emissão do certificado, bem como informar o motivo da revogação.

4.4.3.2. Como diretrizes gerais, fica estabelecido:

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

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

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

d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC.

4.4.3.3. O prazo máximo admitido para a conclusão do processo de revogação de certificado emitido pela AC VALID RFB, 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 VALID RFB responde plenamente por todos os danos causados pelo uso do certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.4.3.6. 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. O prazo para aceitação do certificado pelo titular é de 2 (dois) dias úteis, dentro desse prazo a revogação do certificado pode ser solicitada sem ônus.

4.4.4.2. Não se aplica.

4.4.5. Circunstâncias para suspensão

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

4.4.6. Quem pode solicitar suspensão

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

4.4.7. Procedimento para solicitação de suspensão

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

4.4.8. Limites no período de suspensão

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

4.4.9. Frequência de emissão de LCR

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

4.4.9.2. A frequência máxima admitida para a emissão de LCR 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 Certificados Revogados

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

4.4.10.2. A autenticidade da LCR/OCSP deverá também ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

4.4.11. Disponibilidade para revogação ou 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 VALID RFB dispõe de recursos para verificação de status on-line de certificados, quando aplicável por força de contratação específica. A verificação da situação de um certificado poderá ser feita diretamente na AC VALID RFB, por meio do protocolo OCSP (*On-line Certificate Status Protocol*).

4.4.12. Requisitos para verificação de revogação *on-line*

Não se aplica.

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. Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deve notificar imediatamente a AC VALID RFB, solicitando a revogação de seu certificado através do formulário específico para tal fim. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.4.15.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente numa das instalações técnicas onde realizou a validação presencial, assinando formulário de solicitação de revogação, observado o previsto no item 4.4.3.

4.4.15.3. Todos os documentos e relatórios relativos a esse processo são arquivados após sua conclusão.

4.5. Procedimentos de Auditoria de Segurança

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

4.5.1. Tipos de eventos registrados

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

a) Iniciação e desligamento do sistema de certificação;

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

c) Mudanças na configuração da AC VALID 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 VALID RFB ou de chaves de seus usuários finais;

h) Emissão e revogação de certificados;

i) Geração de LCR;

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

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

l) Operações de escrita nesse repositório, quando aplicável.

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

a) Registros de acessos físicos;

b) Manutenção e mudanças na configuração de seus sistemas;

c) Mudanças de pessoal e de perfis qualificados;

d) Relatórios de discrepância e comprometimento; e

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

4.5.1.3. As informações registradas pela AC VALID RFB são todas as descritas nos itens acima.

4.5.1.4. Todo o registro de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a identidade do agente que o causou.

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

4.5.1.6. As ARs vinculadas à AC VALID RFB registram eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são 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 VALID 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*)

A análise dos registros de auditoria é realizada semanalmente pela Área de Segurança e PKI da AC VALID RFB. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando-se que não foram alterados, em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3. Período de retenção para registros (*logs*) de auditoria

A AC VALID RFB mantém localmente, nas suas instalações, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4. Proteção de registro (*log*) de auditoria

4.5.4.1. Os equipamentos da AC VALID RFB, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança. 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. A inspeção contínua dos diversos registros dos sistemas é feita por meio de ferramentas nativas do sistema operacional e do banco de dados. Os relatórios emitidos a partir dessas ferramentas são coletados e armazenados em sala de arquivos em nível 3 de segurança.

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

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

São executados semanalmente os procedimentos de *backup* (cópias de segurança) dos registros de auditoria dos sistemas utilizados pela AC VALID RFB. Essas cópias semanais são feitas automaticamente ou pelos administradores de sistemas e enviadas às Equipe de Segurança e PKI.

4.5.6. Sistema de coleta de dados de auditoria

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

4.5.7. Notificação de agentes causadores de eventos

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

4.5.8. Avaliações de vulnerabilidade

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

4.6. Arquivamento de Registros

4.6.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC VALID RFB:

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC VALID RFB; e

g) Informações de auditoria previstas no item 4.5.1.

4.6.2. Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são:

a) As LCRs e os certificados de assinatura digital deverão ser 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. *As prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado*; e

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

4.6.3. Proteção de arquivo

Todos os registros são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme 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 deverá ser armazenada em local externo à AC VALID RFB, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

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

4.6.5. Requisitos para datação de registros

Os servidores estão sincronizados com a Fonte Confiável de Tempo da AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário da Fonte Confiável de Tempo da AC Raiz, inclusive os certificados emitidos por esses equipamentos.
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

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

4.6.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC VALID RFB, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado. Não serão disponibilizadas informações sigilosas para verificação.

4.7. Troca de chave

4.7.1. Trinta dias antes da expiração do certificado digital, a AC VALID RFB ou a AR vinculada, através do e-mail cadastrado no formulário de solicitação de certificado, informa ao titular a data de expiração e as instruções para a solicitação de um novo certificado.

4.7.2. Não se aplica.

4.8. Comprometimento e Recuperação de Desastre

Os procedimentos de notificação e de recuperação de desastres, para garantir a continuidade dos serviços críticos, estão descritos no Plano de Continuidade de Negócio (PCN) da AC VALID RFB, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Esse PCN, de caráter sigiloso, é testado pelo menos uma vez por ano.

4.8.1. Recursos computacionais, software e dados corrompidos

O PCN especifica as ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

a) é feita a identificação de todos os elementos corrompidos;

b) o instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;

c) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um backup de segurança até a revogação do certificado da AC VALID RFB.

4.8.2. Certificado de entidade é revogado

O PCN especifica as ações a serem tomadas no caso em que o certificado da AC VALID RFB for revogado, as quais se resumem no seguinte:

a) em caso de revogação do certificado da AC VALID RFB, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora.

b) a seguir são revogados todos os certificados emitidos pela das AC VALID RFB. É gerado novo par de chaves da AC VALID RFB, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado. A AC VALID RFB emite então novos certificados digitais para os usuários finais que tiveram seus certificados revogados nesta situação.

4.8.3. Chave de entidade é comprometida

O PCN especifica as ações a serem tomadas no caso em que a chave privada da AC VALID RFB for comprometida, e que se resumem no seguinte:

a) em caso de comprometimento da chave da AC VALID RFB, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora.

b) na confirmação do incidente, são revogados os certificados da AC VALID RFB e os certificados por ela emitidos. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado da AC VALID RFB. A seguir são emitidos, pela AC VALID RFB, novos certificados digitais para os usuários finais que tiveram seus certificados revogados nesta situação.

4.8.4. Segurança dos recursos após desastre natural ou de outra natureza

O PCN especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza, como fogo, greves etc. e que podem ser resumidas no seguinte:

a) é feita a identificação da crise e o acionamento das equipes envolvidas;

b) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas;

c) confirmado o desastre e constatada a impossibilidade de operação no site principal, as atividades são transferidas para o site de contingência.

4.8.5. Atividades das Autoridades de Registro

O PCN das ARs Vinculadas contempla os procedimentos para recuperação total ou parcial das atividades da AR, entre os quais:

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 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. A AC VALID RFB observa os procedimentos descritos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], este item descreve os requisitos e procedimentos adotados nos casos de extinção dos serviços da AC VALID RFB ou de uma AR ou PSS a ela vinculados.

4.9.2. Quando for necessário encerrar as atividades da AC VALID RFB ou da AR VALID, 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 VALID RFB e AR VALID;

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 VALID RFB e pelas ARs vinculadas para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1. Controles Físicos

5.1.1. Construção e localização das instalações da AC VALID RFB

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

5.1.1.2. Nas instalações da AC VALID RFB, foram implementados, entre outros, os seguintes controles de segurança física:

a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, 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; e

d) Iluminação de emergência.

5.1.2. Acesso físico nas instalações da AC VALID RFB

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

5.1.2.1. Níveis de acesso

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

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

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido no ambiente onde estão instalados os equipamentos utilizados na operação da AC VALID RFB, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro nível. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas por meio eletrônico e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC VALID RFB.

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

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

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

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

5.1.2.1.9. No quarto nível, todas as paredes, o piso e o teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem a chamada sala-cofre – possuem proteção contra interferência eletromagnética externa.

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

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

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

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

a) é feito em aço;

b) possui tranca com chave.

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 fechadura individual. Os dados de ativação da AC VALID RFB estão 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. As mídias de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 1 (um) ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da mídia) pelo menos a cada 3

(três) meses, com a escolha de, no mínimo, 1 (uma) mídia referente a cada semana. Essas mídias são armazenadas em ambiente de terceiro nível.

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

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

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

5.1.2.2.6. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, é permanentemente monitorado por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações do guardo.

5.1.2.3. Sistema de controle de acesso

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

5.1.2.4. Mecanismos de emergência

5.1.2.4.1. Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC VALID RFB em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

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

5.1.3. Energia e ar condicionado nas instalações da AC VALID RFB

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

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

5.1.3.3. São 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. São utilizados dutos separados para os cabos de energia, de telefonia e de dados.

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

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

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

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

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

5.1.3.9. O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

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

a) Geradores de porte compatível;

b) Geradores de reserva;

c) Sistemas de *no-breaks* redundantes; e

d) Sistemas redundantes de ar condicionado.

5.1.4. Exposição à água nas instalações da AC VALID RFB

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

5.1.5. Prevenção e proteção contra incêndio nas instalações da AC VALID RFB

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 VALID RFB não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. A sala-cofre de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só deverá se abrir quando a anterior estiver fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC VALID 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 da AC VALID RFB

A AC VALID RFB responsável atende a norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

5.1.7. Destruição de lixo nas instalações da AC VALID RFB

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

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

5.1.8. Instalações de segurança (*backup*) externas (*off-site*) para a AC VALID RFB

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

5.1.9. Instalações técnicas de AR

As instalações técnicas de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

5.2. Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC VALID RFB e nas ARs vinculadas, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, deve também ser estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. A AC VALID RFB adota uma política de separação de funções críticas, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

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

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

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

5.2.2. Número de pessoas necessário por tarefa

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

5.2.2.2. Todas as tarefas executadas no ambiente onde estiver localizado o equipamento de certificação da AC VALID RFB necessitam da presença de, no mínimo, 2 (dois) de seus operadores com perfis qualificados. As demais tarefas da AC poderão ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

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

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

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

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

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

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

a) Ser diretamente atribuídos a um único empregado (funcionário da AC VALID RFB devidamente qualificado);

b) Não são compartilhados; e

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

5.2.3.3. A AC VALID RFB deverá implementar um padrão de utilização de “senhas fortes”, definido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes estão descritos os requisitos e procedimentos implementados pela AC VALID RFB, pelas ARs e PSSs vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os empregados da AC VALID RFB e das ARs e PSSs vinculados, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

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

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

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 VALID RFB e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido Política de Segurança da AC VALID RFB e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.2. Procedimentos de verificação de antecedentes

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

a) Verificação de antecedentes criminais;

b) Verificação de situação de crédito;

c) Verificação de histórico de empregos anteriores; e

d) Comprovação de escolaridade e de residência.

5.3.2.2. Não se aplica.

5.3.3. Requisitos de treinamento

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

a) Princípios e mecanismos de segurança da AC VALID RFB e das ARs vinculadas;

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

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

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 VALID RFB e das ARs vinculadas, 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 VALID RFB ou das ARs.

5.3.5. Frequência e sequência de rodízio de cargos

A AC VALID RFB não implementa rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

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

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

a) Relato da ocorrência com "*modus 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 VALID RFB encaminhará suas conclusões à AC Raiz.

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

a) Advertência;

b) Suspensão por prazo determinado; ou

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

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da AC VALID RFB e das ARs vinculadas, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados será contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e na Política de Segurança da AC VALID RFB.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC VALID RFB disponibilizará para todo o seu pessoal e para o pessoal das ARs vinculadas:

a) Esta DPC;

b) As PCs que implementa;

c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];

d) Documentação operacional relativa a suas atividades;

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

f) A Política de Segurança da AC VALID RFB.

5.3.8.2. Toda a documentação fornecida ao pessoal é classificada segundo a política de classificação de informação definida pela AC VALID RFB e 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 da AC VALID RFB é gerado pela própria AC VALID RFB, em módulo criptográfico de *hardware* com padrão de segurança após pedido e deferimento do credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. A geração do par de chaves da AC VALID RFB é feita em processo verificável, feito na presença de funcionários de confiança e treinados para a função, somente pelo titular do certificado correspondente.

6.1.1.3. As PCs implementadas pela AC VALID RFB definem o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.2. 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. A AC VALID RFB entrega cópia de sua chave pública para a Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) em formato PKCS#10. Essa entrega é feita por representante legal constituído da AC VALID RFB, em cerimônia especifica, em data e hora previamente estabelecida.

6.1.3.2. Chaves públicas de usuários finais são entregues à AC VALID RFB por meio de uma troca on-line utilizando funções automáticas do software de certificação da AC VALID RFB. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4. Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC VALID RFB compreendem:

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

b) Diretório;

c) Página web da AC VALID RFB: http://www.validcertificadora.com.br/ac-valid-rfb ; e

d) Outros meios seguros aprovados pelo Comitê Gestor da ICP-Brasil.

6.1.5. Tamanhos de chave

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

6.1.5.2. Não se aplica.

6.1.6. Geração de parâmetros de chaves assimétricas

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

6.1.7. Verificação da qualidade dos parâmetros

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

6.1.8. Geração de chave por *hardware* ou *software*

6.1.8.1. Para geração de seus pares de chaves, a AC VALID RFB utiliza componentes seguros de hardware, que possuem mecanismos de prevenção e detecção de violação.

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

6.1.9. Propósitos 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 VALID 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 VALID RFB é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCRs.

6.2. Proteção da Chave Privada

As chaves privadas da AC VALID 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.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC VALID RFB adota o padrão de Homologação da ICP-Brasil NSH-2. Este padrão está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Nos certificados de titulares finais, esses devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]. Cada PC implementada especifica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.2.2. Controle "n de m" para chave privada

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

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

6.2.3. Recuperação (*escrow*) de chave privada

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

6.2.4. Cópia de segurança (backup) de chave privada

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

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

6.2.4.3. A AC VALID RFB não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC VALID RFB poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido. Cada PC implementada defini os requisitos específicos aplicáveis.

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. As chaves privadas dos titulares de certificados emitidos pela AC VALID RFB não são arquivadas.

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

6.2.6. Inserção de chave privada em módulo criptográfico

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

6.2.7. Método de ativação de chave privada

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

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

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

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

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

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos titulares dos certificados de assinatura digital emitidos pela AC VALID RFB são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

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

6.3.2.4. A validade admitida para certificados da AC VALID 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 da chave privada da AC VALID RFB são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em hardware (cartão criptográfico).

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 das chaves privadas da AC VALID RFB são protegidos contra uso não autorizado por meio de mecanismo 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 o 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 VALID RFB é realizada em ambiente computacional, mantido *off-line* de modo a impedir o acesso remoto não autorizado.

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

6.5.1.3. Os computadores servidores da AC VALID RFB, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, Contém as seguintes características:

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

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

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

f) Mecanismos para cópias de segurança (*backup*).

6.5.1.4. Essas características são implementadas 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 VALID RFB, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC VALID RFB. Todos esses eventos são registrados para fins de auditoria.

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

6.5.2. Classificação da segurança computacional

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

6.5.3. Controles de Segurança para as Autoridades de Registro

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

6.5.3.2. São incluídos, no mínimo, os requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], tais como:

a) Segurança de Pessoal:

b) Segurança Física;

c) Segurança Lógica;

d) Segurança de Rede; e

e) Segurança da Informação.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistema

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

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

6.6.2. Controles de gerenciamento de segurança

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

a) a AC VALID RFB opera em equipamento fisicamente protegido em ambiente de nível 4;

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

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

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

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

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

d) instalação de novos serviços na plataforma de processamento.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Antes de publicadas, todas as LCRs geradas pela AC VALID 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 VALID RFB, incluindo *firewalls* e recursos similares.

6.7.1.2. Nos servidores do sistema de certificação da AC VALID 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 VALID 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. O *firewall* promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC VALID RFB.

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

6.7.3. Sistema de detecção de intrusão (IDS)

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

6.7.3.2. O sistema de detecção de intrusão reconhece 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 diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela AC VALID RFB para o armazenamento de sua chave privada está em conformidade com o padrão FIPS 140-2 nível 3 (para a cadeia de certificação V3) e no padrão obrigatório de Homologação da ICP-Brasil NSH-2 (para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

7. PERFIS DE CERTIFICADO E LCR

7.1. Diretrizes Gerais

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

7.1.2. AC VALID RFB implementa as PCs abaixo, as quais especificam os formatos dos certificados gerados e das correspondentes LCR. Nessas PC são incluídas informações sobre os padrões adotados, seus perfis, versões e extensões:

POLÍTICA DE CERTIFICADO	NOME	OID
Política de Certificado de Assinatura Digital do tipo A1 da AC VALID RFB	PC A1 da AC VALID RFB	2.16.76.1.2.1.37
Política de Certificado de Assinatura Digital do tipo A3 da AC VALID RFB	PC A3 da AC VALID RFB	2.16.76.1.2.3.36

7.1.3. Não se aplica.

7.2. Perfil do Certificado

Todos os certificados emitidos pela AC VALID 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 VALID 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 VALID RFB é 2.16.76.1.1.45.

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 VALID RFB implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2. Extensões de LCR e de suas entradas

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

a) "***Authority Key Identifier***": contém o *hash* SHA-1 da chave pública da AC VALID RFB que assina a LCR;

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

c) "***Authority Information Access***", **não crítica**: contém o método de acesso id-ad-caIssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta DPC da AC VALID RFB será submetida previamente à aprovação do Comitê Gestor da ICP-Brasil. Esta DPC será atualizada sempre que uma nova PC for implementada pela AC VALID RFB o exigir.

8.2. Políticas de publicação e notificação

A AC VALID RFB publica e mantém atualizada esta DPC e PCs, em seu endereço web: http://www.validcertificadora.com.br/ac-valid-rfb .

8.3. Procedimentos de aprovação

Esta DPC foi submetida à aprovação do Comitê Gestor da ICP-Brasil durante o processo de credenciamento da AC VALID RFB, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9. DOCUMENTOS REFERENCIADOS

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

9.2. Os documentos a seguir 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 ARs DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITIMOS 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]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[4]	TERMO DE TITULARIDADE	ADE-ICP-05.B

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 - On-line Certificate Status Protocol
OID - Object Identifier
OU - Organization Unit
PASEP - Programa de Formação do Patrimônio do Servidor Público
PC - Políticas de Certificado
PCN - Plano de Continuidade de Negócio
PIS - Programa de Integração Social
POP - Proof of Possession
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