Declaração de Práticas de Certificação da Autoridade Certificadora Validar Múltipla (DPC AC Validar Múltipla)

OID: 2.16.76.1.1.197

Versão 1.0

Março de 2023

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item alterado	Descrição da alteração
1.0	Março/2023	-	Não há	Versão inicial – Baseada no DOC-ICP-05 Versão 6.3

1. INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP- Brasil.

1.1. Visão Geral

1.1.1. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora AC Validar Múltipla integrante na Infraestrutura de Chaves Públicas Brasileira (ICP- Brasil) na execução dos seus serviços de certificação digital.

1.1.2. A estrutura desta DPC está baseada no DOC-ICP-05.

As referências a formulários presentes nesta DPC deverão ser entendidas também como referências a outras formas que a AC Validar Múltipla possa vir a adotar.

1.1.3. Não se aplica.

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

1.1.5. A AC Validar Múltipla mantém todas as informações da sua DPC sempre atualizadas.

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

1.2. Nome e identificação do documento

1.2.1. Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora Validar Múltipla no âmbito da ICP-Brasil e referida como "DPC da AC Validar Múltipla", cujo **OID** (*object identifier*) é **2.16.76.1.1.197.**

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

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

Esta DPC refere-se exclusivamente à AC Validar Múltipla no âmbito da ICP- Brasil.

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC Validar Múltipla para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC Validar Múltipla (http://syngularid.com.br/repositorio/ac-validar-multipla/):

a) Relação de todas as ARs credenciadas;
b) Relação de AR que tenham se descredenciado da cadeia da AC Validar Múltipla, com respectiva data do descredenciamento.

1.3.3. Titulares do Certificado

Os titulares dos certificados emitidos pela AC Validar Múltipla podem ser pessoas físicas ou jurídicas, de direito público ou privado, nacionais ou estrangeiras, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis, podem ser Titulares de Certificado. Os certificados podem ser utilizados por pessoas físicas, pessoas jurídicas. Em sendo o titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada. Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

1.3.5.1. A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC Validar Múltipla é publicada em serviço de diretório e/ou em página web da AC Validar Múltipla (http://syngularid.com.br/repositorio/ac-validar-multipla/).

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

A AC Validar Múltipla implementa as seguintes Políticas de Certificado Digital: Para Certificados de Assinatura Digital:

i. Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora Validar Múltipla no âmbito da ICP-Brasil, PC A1 da AC Validar Múltipla, OID 2.16.76.1.2.1.157.

ii. Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora Validar Múltipla no âmbito da ICP-Brasil, PC A3 da AC Validar Múltipla, OID 2.16.76.1.2.3.148.

1.4.2. Uso proibitivo do certificado

Quando cabível, as aplicações para as quais existem restrições ou proibições para o uso desses certificados estão listados nas PCs implementadas.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

Esta DPC é administrada pela Validar Múltipla.

1.5.2. Contatos

Endereço: Rua Prefeito Osmar Cunha, 183, sala 1005, Bloco B, Centro, Florianópolis/SC.
CEP: 88.015-900.
Telefone: 48-3028-3700.
Página Web: http://acvalidar.com.br
E-mail: contato@arvalidar.com.br

1.5.3. Pessoa que determina a adequabilidade da DPC com a PC

Nome: CARLOS FRANCISCO TATARA
E-mail: compliance@syngular.id
Telefone: 48 4042-1641.

1.5.4. Procedimentos de aprovação da DPC

Esta DPC é aprovada pela AC Validar Múltipla e pelo ITI.
Os procedimentos de aprovação da DPC da AC Validar Múltipla são estabelecidos a critério do CG da ICP-Brasil.

1.6. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	**Autoridade Certificadora**
AC Raiz	**Autoridade Certificadora Raiz da ICP-Brasil**
AR	**Autoridades de Registro**
CEI	**Cadastro Específico do INSS**
CF-e	**Cupom Fiscal Eletrônico**
CG	**Comitê Gestor**
CN	**Common Name**

CNE	**Carteira Nacional de Estrangeiro**
CNPJ	**Cadastro Nacional de Pessoas Jurídicas**
CPF	**Cadastro de Pessoas Físicas**
DMZ	**Zona Desmilitarizada**
DN	**Distinguished Name**
DPC	**Declaração de Práticas de Certificação**
ICP-Brasil	**Infraestrutura de Chaves Públicas Brasileira**
IDS	**Intrusion Detection System**
IEC	**International Electrotechnical Commission**
IETF PKIX	**Internet Engineering Task Force - Public-Key Infrastructured (X.509)**
ISO	**International Organization for Standardization**
ITU	**International Telecommunications Union**
LCR	**Lista de Certificados Revogados**
NBR	**Norma Brasileira**
NIS	**Número de Identificação Social**
OCSP	**Online Certificate Status Protocol**
OID	**Object Identifier**
OM-BR	**Objetos Metrológicos ICP-Brasil**
OU	**Organization Unit**
PC	**Políticas de Certificado**
PCN	**Plano de Continuidade de Negócio**
PIN	**Personal Identification Number**
PS	**Política de Segurança**
PSBIO	**Prestador de Serviço Biométrico**
PSC	**Prestador de Serviço de Confiança**
PSS	**Prestadores de Serviço de Suporte**
PUK	**PIN Unbloking Key**
RFC	**Request For Comments**
RG	**Registro Geral**
SAT	**Sistema de Autenticação e Transmissão**
SNMP	**Simple Network Management Protocol**
SSL	**Secure Socket Layer**
UF	**Unidade de Federação**
URL	**Uniform Resource Locator**

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1. A AC Validar Múltipla mantém disponível repositório atendendo as seguintes obrigações:

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

b) Estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
c) Implementar os recursos necessários para a segurança dos dados nele armazenados.

2.1.2. Requisitos aplicáveis aos repositórios utilizados pela AC VALIDAR MÚLTIPLA responsável pela DPC:

a) Localização física e lógica;
b) Disponibilidade;
c) Protocolos de acesso;
d) Requisitos de segurança

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

2.1.4. A AC Validar Múltipla disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR.

i. http://syngularid.com.br/repositorio/ac-validar-multipla/lrc/lcr-ac-validar-multipla.crl

ii. http://icp-brasil.syngularid.com.br/repositorio/ac-validar-multipla/lcr/lcr-ac-validar-multipla.crl

2.2. Publicação de informações dos certificados

2.2.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página *web* da AC Validar Múltipla (http://www.syngularid.com.br/repositorio/ac-validar-multipla) regras e os critérios estabelecidos nesta DPC.

A disponibilidade das informações publicadas pela AC Validar Múltipla em serviço de diretório e/ou página *web* é de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2. As seguintes informações são publicadas em serviço de diretório e/ou em página *web* da AC Validar Múltipla (http://syngularid.com.br/repositorio/ac-validar-multipla/)

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; e
f) Uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3. Tempo ou Frequência de Publicação

De modo a assegurar a disponibilização sempre atualizada de seus conteúdos, os certificados são publicados imediatamente após sua emissão; a publicação da LCR se dá conforme o item 4.4.9 da PC correspondente; as versões ou alterações desta DPC e da PC são atualizadas no website da AC Validar Múltipla após aprovação da AC Raiz da ICP-Brasil; e os endereços das AR vinculadas são atualizadas no web site da AC Validar Múltipla.

2.4. Controle de Acesso aos Repositórios

Não há nenhuma restrição ao acesso para consulta a esta DPC, à LCR emitidas pela AC Validar Múltipla, às PC implementadas e aos endereços das AR vinculadas de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC Validar Múltipla verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os diretos de propriedade intelectual de terceiros. A AC reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1. Atribuição de Nomes

3.1.1. Tipos de Nomes

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

3.1.1.2. Não se aplica.

3.1.2. Necessidade de nomes significativos

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

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4. Regras para interpretação de vários tipos de nomes

3.1.4.1. Não se aplica.

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

3.1.5. Unicidade de nomes

Os identificadores "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado emitido pela AC Validar Múltipla. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6. Procedimento para resolver disputa de nomes

A AC Validar Múltipla 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.

3.2. Validação Inicial de Identidade

Neste item e nos seguintes, a DPC descreve detalhes os requisitos e procedimentos utilizados pelas ARs vinculadas à AC Validar Múltipla para a realização dos seguintes processos:

a) Identificação do titular do certificado – identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2 e 3.2.3 observando quanto segue:

   i. Para certificados de pessoa física: comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim.

   ii. Para certificados de pessoa jurídica: comprovação de que os documentos apresentados se referem efetivamente à pessoa jurídica titular do certificado, e de

que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.

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

3.2.1. Método para comprovar o controle de chave privada

A AC Validar Múltipla verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. Para esta finalidade é utilizada como referências a RFC 4210, atualizada pela 6712.

3.2.2. Autenticação da identificação da organização

3.2.2.1. Disposições Gerais

3.2.2.1.1. Neste item estão definidos os procedimentos empregados pelas ARs vinculadas para a confirmação da identidade de uma pessoa jurídica.

3.2.2.1.2. Será designado como responsável pelo certificado o representante legal da pessoa jurídica requerente do certificado, ou o procurador constituído na forma do item 3.2, alínea 'a', inciso (ii) acima, o qual será o detentor da chave privada.

3.2.2.1.3. 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 3.2.2.2;
b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
c) coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil, bem como os procedimentos para identificação biométrica na ICP-Brasil; e
d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo responsável pelo certificado.

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

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

3.2.2.1.5. O disposto no item 3.2.2.1.3 poderá ser realizado:

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

3.2.2.2. Documentos para 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 CNPJ;
    ii. se entidade privada:
        1. certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e
        2. documentos da eleição de seus representantes legais, quando aplicável.
b) Relativos à sua habilitação fiscal:
    i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
    ii. prova de inscrição no Cadastro Específico do INSS – CEI.

Nota 1: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

3.2.2.3. Informações contidas no certificado emitido para uma organização.

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

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

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

3.2.2.4. Responsabilidade decorrente do uso do certificado de uma organização.

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

3.2.3. Autenticação da identidade de um indivíduo

A confirmação deverá ser realizada mediante a presença física do interessado ou por um dos procedimentos listados nas alíneas abaixo, que asseguram nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico:

a) Não se aplica;
b) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz; ou
c) Não se aplica.

3.2.3.1. Documentos para efeitos de identificação de um indivíduo

A identificação da pessoa física requerente do certificado deverá ser realizada como segue:

a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:
i. Registro de Identidade, se brasileiro; ou
ii. Título de Eleitor, com foto; ou
iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
iv. Passaporte, se estrangeiro não domiciliado no Brasil.
b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução

Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

Nota 1: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

3.2.3.1.1. Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a apresentação de qualquer dos documentos elencados no item 3.2.3.1 e da etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

3.2.3.1.2. Os documentos digitais deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos. Tal verificação fará parte do dossiê eletrônico do titular do certificado. Na hipótese da identificação positiva, fica dispensada a etapa de verificação conforme o item 3.2.3.1.3.

3.2.3.1.3. Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados:

a) por agente de registro distinto do que realizou a etapa de identificação;
b) na sede da AR ou AR própria da AC ou ainda AR própria do PSS da AC; e
c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.2.3.1.4. A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente, e as normas editadas pelo Comitê Gestor da ICP-Brasil.

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7. Não se aplica.

3.2.3.1.8. A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICP-Brasil, que deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade.

3.2.3.1.8.1. Não se aplica.

3.2.3.2. Informações contidas no certificado emitido para um indivíduo

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

a) Nome completo, sem abreviações;
b) Data de nascimento; e
c) Cadastro de Pessoa Física (CPF).

3.2.3.2.1.1. Não se aplica.

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

a) Número de Identificação Social - NIS (PIS, PASEP ou CI);
b) Número do Registro Geral - RG do titular e órgão expedidor;
c) Número do Cadastro Específico do INSS (CEI) ou CAEPF;
d) Número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do título de Eleitor; e
e) Número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

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

3.2.3.2.3.1. Não se aplica.

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.

3.2.4. Informações não verificadas do titular do certificado

Não se aplica.

3.2.5. Validação das autoridades

Não se aplica.

3.2.6. Critérios para interoperação

Não se aplica.

3.2.7. Autenticação da identidade de equipamento ou aplicação

3.2.7.1. Disposições Gerais

3.2.7.1.1. Não se aplica.

3.2.7.1.2. Não se aplica.

3.2.7.1.3. Não se aplica.

3.2.7.1.4. Não se aplica.

3.2.7.1.5. Não se aplica.

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

3.2.7.2.1. Não se aplica.

3.2.7.2.2. Não se aplica.

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

3.2.7.3.1. Não se aplica.

3.2.7.3.2. Não se aplica.

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

3.2.7.4.1. Disposições gerais.

3.2.7.4.1.1. Não se aplica.

3.2.7.4.1.2. Não se aplica.

3.2.7.4.1.3. Não se aplica.

3.2.7.5. Procedimentos para efeitos de identificação de um equipamento SAT

Não se aplica.

3.2.7.6. Informações contidas no certificado emitido para um equipamento SAT

3.2.7.6.1. Não se aplica.

3.2.7.6.2. Não se aplica.

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

3.2.7.7.1. Disposições gerais.

3.2.7.7.1.1. Não se aplica.

3.2.7.7.1.2. Não se aplica.

3.2.7.7.1.3. Não se aplica.

3.2.7.8. Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

3.2.7.9. Informações contidas no certificado emitido para um equipamento metrológico.

3.2.7.9.1. Não se aplica.

3.2.7.9.2. Não se aplica.

3.2.8. Procedimentos complementares

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

3.2.8.2. Todo o processo de identificação do titular do certificado deve ser registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC Validar Múltipla, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. O sistema biométrico da ICP-BRASIL deve solicitar aleatoriamente qual dedo o AGR deve apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGR no cadastro do sistema biométrico. Tais registros devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.2.8.2.1. Não se aplica.

3.2.8.3. É mantido arquivo eletrônico 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].

3.2.8.3.1. Não se aplica.

3.2.8.3.2. Não se aplica.

3.2.8.3.3. Não se aplica.

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

3.2.8.4.1. Na hipótese de identificação positiva no processo biométrico da ICP- Brasil, fica dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação conforme item 3.2.3.1.

3.2.8.4.2. Não se aplica.

3.2.9. Procedimentos específicos

3.2.9.1. Não se aplica.

3.2.9.2. Não se aplica.

3.2.9.3. Não se aplica.

3.2.9.3.1. Módulo Eletrônico da AR dos Órgãos Gestores de Pessoas

Não se aplica.

3.2.9.3.2. Não se aplica.

3.2.9.3.3. Não se aplica.

3.2.9.3.4. Não se aplica.

3.2.9.4. Não se aplica.

3.2.9.4.1. Não se aplica.

3.2.9.5. Disposições para a Validação de Solicitação de Certificados do Tipo OM-BR

Não se aplica.

3.2.9.6. Não se aplica.

3.2.9.7. Não se aplica.

3.2.9.8. Não se aplica.

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. Esta DPC estabelece os processos de Identificação e confirmação do cadastro do solicitante, utilizados pele AC Validar Múltipla para a geração de novo par de chaves e de seu correspondente certificado, antes da expiração de um certificado vigente.

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

a) Adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;
b) Solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil valido, do tipo A3, que seja pelo menos do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física:
c) Solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;
d) Solicitação por meio eletrônico dada nas alíneas 'b' e 'c', acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação da AC-Raiz ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;
e) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou
f) Não se aplica.

3.3.2.1. Não se aplica.

3.3.3. Não existem procedimentos específicos para as PCs.

3.3.4. Não se aplica.

3.4. Identificação e Autenticação para solicitação de revogação

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo

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 Validar Múltipla está descrito no item 4.9.3. Todas as solicitações de revogação de certificados devem ser registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. Solicitação de Certificado por videoconferência e outras formas tradicionais.

Para atender à solicitação de certificado digital à AC Validar Múltipla e suas ARs vinculadas, os requisitos e procedimentos deverão compreender, no mínimo:

a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
b) O uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; e
c) Um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico;

Nota 1: Não se aplica.

Nota 2: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados de aplicação, equipamento ou outros que façam uso de CSR) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

4.1.1. Quem pode submeter uma solicitação de certificado

A submissão da solicitação deve ser sempre por intermédio da AR a pedido do titular do certificado digital.

4.1.1.1. Não se aplica.

4.1.1.2. Não se aplica.

4.1.1.3. Não se aplica.

4.1.1.4. Não se aplica.

4.1.2. Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas. Caso haja obrigações específicas para as PCs implementadas, as mesmas devem ser descritas nessas PCs, no item correspondente.

4.1.2.1. Responsabilidades da AC

4.1.2.1.1. A AC Validar Múltipla responde pelos danos a que der causa.

4.1.2.1.2. A AC Validar Múltipla responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

4.1.2.1.3. Não se aplica.

4.1.2.2. Obrigações da AC

As obrigações da AC Validar Múltipla são as abaixo relacionadas:

a) Operar de acordo com a sua DPC e com as PCs que implementa;
b) Gerar e gerenciar os seus pares de chaves criptográficas;
c) Assegurar a proteção de suas chaves privadas;
d) Notificar 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 AR a ela vinculadas e 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 on-line de situação do certificado (OCSP - *On-line Certificate Status Protocol*);
k) Publicar em sua página web sua DPC e as PCs aprovadas que implementa;

l) Publicar, em sua página web, as informações definidas no item 2.2.2 deste documento;
m) Publicar, em página *web*, informações sobre o descredenciamento de AR;
n) Utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web;*
o) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) Adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
q) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
r) Manter e garantir 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, quando esta estiver obrigada a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
u) Informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
v) Informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;
w) Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
x) Realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada e;
y) Garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados.

4.1.2.3. Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

4.1.2.4. Obrigações das ARs

As obrigações das ARs vinculadas à AC Validar Múltipla são as abaixo relacionadas:

a) Receber solicitações de emissão ou de revogação de certificados;
b) Confirmar a identidade do solicitante e a validade da solicitação;
c) Encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC Validar Múltipla 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) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC Validar Múltipla e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP- BRASIL [1], bem como Princípios e Critérios WebTrust para AR [5];
f) Manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;
g) Proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2 e 3.2.3; e
h) Divulgar suas práticas, relativas a cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios *WebTrust* para AR [5].

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

A AC Validar Múltipla e AR executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2. Aprovação ou rejeição de pedidos de certificado

4.2.2.1. Não se aplica.

4.2.2.2. A AC Validar Múltipla e AR podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

4.2.3. Tempo para processar a solicitação de certificado

A AC Validar Múltipla cumpre os procedimentos determinados na ICP-Brasil.

Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

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

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

4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado

O Titular é notificado da emissão e do método para a retirada do certificado.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

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

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

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

4.4.1.3. Não há termos de acordo ou instrumentos similares requeridos pela AC VALIDAR MÚLTIPLA.

4.4.2. Publicação do certificado pela AC

O certificado da AC Validar Múltipla é publicado de acordo com item 2.2 desta DPC.

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

Não se aplica.

4.5. Usabilidade do par de chaves e do certificado

O titular do certificado para usuário final opera de acordo com a Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementam, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.1.1. O titular do certificado digital deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto nesta DPC.

4.5.1.2. Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos pela AC Validar Múltipla constantes dos termos de titularidade de que trata o item 4.1 são os abaixo relacionados:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, código de ativação (PIN) e dispositivos criptográficos;
c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;
e) informar à AC Validar Múltipla qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente; e
f) garantir a proteção do PUK, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente.

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

4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Em acordo com o item 3.3 desta DPC

4.6.1. Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2. Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3. Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4. Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com item 3.3 desta DPC.

4.6.6. Publicação de uma renovação de um certificado pela AC

Não se aplica.

4.6.7. Notificação de emissão de certificado pela AC para outras entidades

Em acordo com item 4.3 desta DPC.

4.7. Nova chave de certificado (*Re-key*)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica.

4.7.2. Quem pode requisitar a certificação de uma nova chave pública

Não se aplica.

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica.

4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica.

4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades

Não se aplica.

4.8. Modificação de certificado

Não se aplica.

4.8.1. Circunstâncias para modificação de certificado

Não se aplica.

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6. Publicação de uma modificação de certificado pela AC

Não se aplica.

4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades

Não se aplica.

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

4.9.1.1. O titular e o responsável pelo certificado podem solicitar a revogação de seu certificado a qualquer tempo, independentemente de qualquer circunstância.

4.9.1.2. O certificado deve ser obrigatoriamente revogado:

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

4.9.1.3. A AC Validar Múltipla define ainda que:

a) A AC Validar Múltipla deve revogar, no prazo definido no item 4.9.3.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
b) O CG da ICP-Brasil ou 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.

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

4.9.1.4.1. Não se aplica.

4.9.1.4.2. Não se aplica.

4.9.1.5. A autenticidade da LCR é também confirmada por meio das verificações da assinatura da AC Validar Múltipla emitente e do período de validade da LCR.

4.9.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) Por solicitação do titular do certificado;
b) Por solicitação do responsável pelo certificado, no caso de 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 Validar Múltipla emitente;
e) Por uma AR vinculada;
f) Por determinação da AC SyngularID, do CG da ICP-Brasil ou da AC Raiz; ou
g) Não se aplica;
h) Não se aplica;
i) Não se aplica;
j) Não se aplica.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. Uma solicitação de revogação é necessária para que AR responsável inicie o processo de revogação. O solicitante da revogação habilitado pode solicitar facilmente e a qualquer tempo a revogação de certificado, evitando assim a utilização indevida do certificado.

Instruções para a solicitação de revogação do certificado são obtidas em página web disponibilizada pela AC Validar Múltipla ou pela AR Responsável.

A revogação é realizada através de Formulário on-line contendo o motivo da solicitação de revogação mediante o fornecimento de dados e da frase de identificação indicada na solicitação de emissão do Certificado.

Caso o Titular ou o Responsável - no caso de certificados de pessoas jurídicas ou aplicações - não recorde a frase de identificação ou quando a revogação é solicitada diretamente pelo Titular sem a participação do Responsável, o Formulário de revogação é impresso e assinado e entregue na AR Responsável.

4.9.3.2. Como diretrizes gerais:

a) O Solicitante da revogação de um certificado é identificado;
b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC Validar Múltipla;
c) As justificativas para a revogação de um certificado são registradas;
d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.9.3.3. O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos ostipos de certificado previstos pela ICP-Brasil

é de 24 (vinte e quatro) horas.

4.9.3.4. Não se aplica.

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

4.9.3.6. Os procedimentos de revogação de certificados estão descritos nas PCs implementadas.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 desta DPC.

O prazo para aceitação do certificado pelo seu titular é de 7 (sete) dias, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

4.9.4.2. Não se aplica.

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

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

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7. Frequência de emissão de LCR

4.9.7.1. A frequência para a emissão de LCR da AC Validar Múltipla referente a certificados de usuários finais é de 6 horas.

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

4.9.7.3. Não se aplica.

4.9.7.4. Não se aplica.

4.9.7.5. Não se aplica.

4.9.8. Latência máxima para a LCR

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

4.9.9. Disponibilidade para revogação/verificação de status on-line

Não se aplica.

4.9.10. Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11. Outras formas disponíveis para divulgação de revogação

4.9.11.1. Não se aplica.

4.9.11.2. Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. O titular de certificado deve notificar imediatamente, através de solicitação on-line de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.9.12.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente na AR Responsável, assinando formulário de solicitação de revogação, observado o item 4.4.3 desta DPC.

Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

4.9.13. Circunstâncias para suspensão

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

4.9.14. Quem pode solicitar suspensão

A AC Validar Múltipla pode solicitar suspensão quando aprovado pelo Comitê Gestor.

4.9.15. Procedimento para solicitação de suspensão

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

4.9.16. Limites no período de suspensão

Os períodos de suspensão serão estabelecidos por norma específica das DPC e PCs associadas.

4.10. Serviços de status de certificado

4.10.1. Características operacionais

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

4.10.2. Disponibilidade dos serviços

Ver item 4.9

4.10.3. Funcionalidades operacionais

Ver item 4.9

4.11. Encerramento de atividades

4.11.1. Observado o disposto no item sobre descredenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], este item da DPC descreve os requisitos e os procedimentos que deverão ser adotados nos casos de extinção ou encerramento dos serviços da AC Validar Múltipla, de uma AR, PSS ou PSBios a ela vinculados.

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

a) Comunicará publicamente a extinção dos serviços da AC Validar Múltipla, através de publicação em jornal de grande circulação.
b) Revogará todos os certificados gerados pela AC Validar Múltipla nos prazos estipulados nas PC implementadas após a publicação e comunicará às partes afetadas através de mensagem eletrônica.
c) Extinguirá os serviços de emissão de certificados.
d) Extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços

de status on-line após a revogação completa de todos os certificados.

e) Destruirá a chave privada da AC Validar Múltipla extinta seguindo o procedimento descrito na DPC Item 6.2.9.
f) Transferirá os dados e gravações da AC Validar Múltipla para a Autoridade Certificadora sucessora, aprovada pela AC Raiz.
g) Transferirá as chaves públicas dos certificados emitidos pela AC Validar Múltipla para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC Validar Múltipla. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.
h) Responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC Validar Múltipla.
i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

A AC Validar Múltipla não executa práticas de custódia e recuperação de chaves.

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

A AC Validar Múltipla não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1. Controles Físicos

5.1.1. Construção e localização das instalações

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

5.1.1.2. Aspectos de construção das instalações da AC Validar Múltipla, relevantes para os controles de segurança física, compreendendo entre outros:

a) As 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 ficam em ambiente seguro;

b) As instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada;
c) Existem sistemas de aterramento e de proteção contra descargas atmosféricas;
d) Existe iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

5.1.2. Acesso físico

A AC Validar Múltipla possui sistema de controle de acesso físico que garante a segurança de suas instalações conforme a POLÍTICA DE SEGURANÇA DA ICP- BRASIL [8] e os requisitos que seguem.

5.1.2.1. Níveis de Acesso

5.1.2.1.1. A AC Validar Múltipla possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC Validar Múltipla.

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC Validar Múltipla. 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 Validar Múltipla transitam devidamente identificadas e acompanhadas.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC Validar Múltipla em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente são utilizados mediante autorização formal e supervisão.

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

5.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC Validar Múltipla. Qualquer atividade relativa ao ciclo de vida dos certificados digitais é executada a partir desse nível. Pessoas não envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6. No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: 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 Validar Múltipla, não são admitidos a partir do

nível 3.

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Validar Múltipla 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, inclusive o sistema de AR. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, 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 sendo ocupado.

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

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

5.1.2.1.11. Na AC Validar Múltipla, existem ambientes de quarto nível para abrigar e segregar, quando for o caso:

a) equipamentos de produção on-line, gabinete reforçado de armazenamento;
b) equipamentos de produção off-line e cofre de armazenamento; e
c) equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores.

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

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

a) confeccionado em aço;
b) possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre (Nível 5). Cada um desses depósitos dispõe de 2 fechaduras, sendo uma individual e a outra comum a todos os depósitos. Os dados de ativação da chave privada da AC Validar Múltipla são armazenados nesses depósitos.

5.1.2.2. Sistemas físicos de detecção

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

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) trimestralmente, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados 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 o critério mínimo de ocupação deixa de ser satisfeito, devido à saída de um ou mais empregados, 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 estão localizados em ambiente de nível 3 e são permanentemente monitorados. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações.

5.1.2.3. Sistema de Controle de Acesso.

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

5.1.2.4. Mecanismos de emergência

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

5.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência 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

5.1.3.1. A infraestrutura do ambiente de certificação da AC Validar Múltipla está 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 Validar Múltipla e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC Validar Múltipla.

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

5.1.3.3. Existem 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, telefonia e dados.

5.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

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

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

5.1.3.7. O sistema de climatização atende aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante às 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 Validar Múltipla é garantida, por meio de:

a) Geradores de porte compatível;
b) Geradores de reserva;
c) Sistemas de "*no-breaks*" redundantes;
d) Sistemas redundantes de ar-condicionado.

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio

5.1.5.1. 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 Validar Múltipla 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 abre quando a anterior estiver fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC Validar Múltipla, a temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.6. Armazenamento de mídia

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

5.1.7. Destruição de lixo

5.1.7.1. Todos os 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*)

As instalações de *backup* deverão atender aos requisitos mínimos estabelecidos por este documento. Sua localização deverá ser tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não sejam atingidas e tornem-se totalmente operacionais em condições idênticas em, no máximo, 48 (quarenta e oito) hora.

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.1.1. A AC Validar Múltipla pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico às funções críticas do ciclo de vida dos certificados digitais, de forma a garantir a segurança da atividade de certificação e evitar a manipulação desautorizada do sistema. As ações permitidas são limitadas de acordo com o perfil de cada cargo.

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

5.2.1.3. Os operadores do sistema de certificação da AC Validar Múltipla recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão determinados, em documento formal (Política de Segurança da AC Validar Múltipla), com base nas necessidades de cada perfil.

5.2.1.3.1. Não se aplica.

5.2.1.4. A AC Validar Múltipla possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos seus funcionários. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o funcionário devolve à AC Validar Múltipla 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 Validar Múltipla, conforme o descrito em 6.2.2.

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

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC Validar Múltipla tem sua identidade e perfil verificados antes de:

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

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

a) são diretamente atribuídos a um único empregado;
b) não são compartilhados; e
c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC Validar Múltipla implementa um padrão de utilização de "senhas fortes", definido em conformidade com a Política de Segurança da ICP-Brasil, junto a procedimentos de validação dessas senhas.

5.2.4. Funções que requerem separação de deveres

AC Validar Múltipla implementa a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3. Controles de Pessoal

Todos os empregados da AC Validar Múltipla, das AR e PSS vinculados encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

a) Os termos e as condições do perfil que ocupam;
b) O compromisso de observar as normas, políticas e regras aplicáveis da AC Validar Múltipla;
c) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
d) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC Validar Múltipla e das AR vinculadas envolvido em atividades diretamente relacionada com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme estabelecido 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 das entidades, todo o pessoal da AC Validar Múltipla e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser submetido a:

a) Verificação de antecedentes criminais;
b) Verificação de situação de crédito;
c) Verificação de histórico de empregos anteriores;
d) Comprovação de escolaridade e de residência.

5.3.2.2. Não se aplica.

5.3.3. Requisitos de treinamento

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

a) Princípios e mecanismos de segurança da AC Validar Múltipla e das ARs vinculadas;
b) Sistema de certificação em uso na AC Validar Múltipla;
c) Procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma dos itens 3.2.2 e 3.2.3; e
e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

O pessoal da AC Validar Múltipla e das AR 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 Validar Múltipla.

5.3.5. Frequência e sequência de rodízios de cargos

Não estabelecido.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Validar Múltipla ou de uma AR vinculada, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, são tomadas as medidas administrativas e legais cabíveis.

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

a) Relato da ocorrência com “modus operandi”;
b) Identificação dos envolvidos;
c) Eventuais prejuízos causados;
d) Punições aplicadas, se for o caso; e
e) Conclusões.

5.3.6.3. Concluído o processo administrativo, a AC Validar Múltipla 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 Validar Múltipla e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC Validar Múltipla disponibiliza para todo o seu pessoal e para o pessoal das ARs vinculadas:

a) A DPC da AC Validar Múltipla;
b) A PC correspondente;
c) A Política de Segurança da AC Validar Múltipla;
d) Documentação operacional relativa às suas atividades; e
e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pela AC Validar Múltipla e é mantida atualizada.

5.4. Procedimentos de Log de Auditoria

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

5.4.1. Tipos de eventos registrados

5.4.1.1. A AC Validar Múltipla registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) Inicialização e desligamento do sistema de certificação;
b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC Validar Múltipla;

c) Mudanças na configuração dos sistemas AC Validar Múltipla 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 do sistema;
g) Geração de chaves próprias da AC Validar Múltipla 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.

5.4.1.1.1. Não se aplica.

5.4.1.2. A AC Validar Múltipla também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

a) Registros de acessos físicos;
b) Manutenção e mudanças na configuração de seus sistemas;
c) Mudanças de pessoal e de perfis qualificados;
d) Relatórios de discrepância e comprometimento; e
e) Registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.3. As informações registradas pela AC Validar Múltipla são todas as descritas nos itens acima.

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

5.4.1.5. A documentação relacionada aos serviços da AC Validar Múltipla é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.1.6. A AC Validar Múltipla registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos 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; e
d) A assinatura digital do executante.

5.4.1.6.1. Não se aplica.

5.4.1.7. A AC Validar Múltipla a que esteja vinculada a AR define, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2. Frequência de auditoria de registros

A periodicidade com que os registros de auditoria da AC Validar Múltipla são analisados pelo pessoal operacional é de uma semana.

Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3. Período de retenção para registros de auditoria

A AC Validar Múltipla mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 5.5.

5.4.4. Proteção de registros de auditoria

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

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

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

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

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC Validar Múltipla têm cópias de segurança semanais, feitas, automaticamente pelo sistema ou

manualmente pelos administradores de sistemas. Estas cópias são enviadas ao departamento de segurança.

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

O sistema de coleta de dados de auditoria interno à AC Validar Múltipla é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.7. Notificação de agentes causadores de eventos

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

5.4.8. Avaliações de vulnerabilidade

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

5.5. Arquivamento de Registros

Nos itens seguintes da DPC está descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC Validar Múltipla e pelas ARs a ela vinculadas.

5.5.1. Tipos de registros arquivados

Os tipos de registros arquivados são:

a) solicitações de certificados;
b) solicitações de revogação de certificados;
c) notificações de comprometimento de chaves privadas;
d) emissões e revogações de certificados;
e) emissões de LCR;
f) trocas de chaves criptográficas da AC Validar Múltipla; e
g) informações de auditoria previstas no item 5.4.1.

5.5.2. Período de retenção para arquivo

Os períodos de retenção por tipo de registro arquivado, são:

a) as LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;

b) os dossiês dos titulares são retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e
c) as demais informações, inclusive os arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

5.5.3. Proteção de arquivo

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

5.5.4. Procedimentos de cópia de arquivo

5.5.4.1. A AC Validar Múltipla estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC Validar Múltipla, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

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

5.5.5. Requisitos para datação de registros

Informações de data e hora nos registros baseiam-se no horário *Greenwich Mean Time* (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero. Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

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

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

5.5.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC Validar Múltipla, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

5.6. Troca de chave

5.6.1. O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico, disponibilizado pela AR Responsável,

por onde é encaminhado o processo de fornecimento de novo certificado.

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

A comunicação de expiração, junto com as instruções para a solicitação de um novo certificado é realizada através de e-mail enviado ao titular do certificado.

5.6.2. Não se aplica.

5.7. Comprometimento e Recuperação de Desastre

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

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

5.7.1.1. A AC Validar Múltipla possui um Plano de Continuidade do Negócio – PCN, de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. Possui ainda um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

5.7.1.2. Os procedimentos previstos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs, contém as seguintes informações:

a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;
b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;
c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários;
d) Documentação dos processos e procedimentos acordados;
e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e
f) Teste e atualização dos planos

5.7.2. Recursos computacionais, software, e/ou dados corrompidos

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da AC Validar Múltipla, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-

determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1. Certificado de entidade é revogado

Em caso de revogação do certificado da AC Validar Múltipla o Gerente de Segurança, junto a Supervisão de PKI da AC Validar Múltipla, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC Validar Múltipla emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

5.7.3.2. Chave de entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC Validar Múltipla, o fato é imediatamente comunicado ao Gerente de Segurança que, junto a Supervisão de AC da AC Validar Múltipla, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

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

5.7.4. Capacidade de continuidade de negócio após desastre

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

a) Garantir a integridade física das pessoas que se encontram nas instalações da AC Validar Múltipla;
b) Monitorar e controlar o foco da contingência;
c) Minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

5.8. Extinção da AC

Conforme CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

6. CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do Par de Chaves

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

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

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

O par de chaves da AC Validar Múltipla é gerado em módulo criptográfico de hardware homologado pela ICP-Brasil conforme definido no DOC-ICP-01.01.

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

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

6.1.1.4. O processo de geração do par de chaves da AC Validar Múltipla é feito por hardware.

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

6.1.1.6. Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC Validar Múltipla são os indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP BRASIL [9].

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Os procedimentos utilizados pela AC Validar Múltipla para a entrega de sua chave pública à AC de nível hierárquico superior encarregada da emissão de seu certificado são definidos pela AC SyngularID.

6.1.3.2. A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - *Secure Socket Layer*. Os procedimentos específicos aplicáveis são detalhados em cada PC implementada.

6.1.4. Entrega de chave pública da AC Validar Múltipla às terceiras partes:

6.1.4.1. As formas para a disponibilização do certificado da AC Validar Múltipla, e de todos os certificados da cadeia de certificação, para os usuários e terceiras partes, as quais poderão compreender, entre outras:

a) No momento da disponibilização de um certificado para seu titular; usando formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil;
b) Diretório: http://syngularid.com.br/repositorio/ac-validar-multipla/certificados/
c) Página web da AC: https://arvalidar.com.br/
d) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Cada PC implementada pela AC Validar Múltipla definirá 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 e verificação da qualidade dos parâmetros

6.1.6.1. Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [1].

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

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

6.1.7.2. A chave privada AC Validar Múltipla é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

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

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

A chave privada da AC Validar Múltipla é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação
Os titulares de certificados emitidos pela AC Validar Múltipla, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado das suas chaves privadas.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC Validar Múltipla adota o padrão de homologação da ICP-Brasil conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICPBrasil.

6.2.1.2. 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 AC Validar Múltipla exige controle múltiplo do tipo “n de m” para ativação da sua chave privada.

6.2.2.2. É necessária a presença de pelo menos 2 (dois) de um grupo de 4 (quatro) funcionários de confiança, com perfis qualificados para a ativação da chave privada da AC Validar Múltipla.

6.2.3. Recuperação (*escrow*) de chave privada

A AC Validar Múltipla não implementa tal prática.

6.2.4. Cópia de segurança (*backup*) de chave privada

6.2.4.1. O titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC Validar Múltipla mantém cópia de segurança de sua chave privada.

6.2.4.3. A AC Validar Múltipla, não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC.

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

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC Validar Múltipla não arquiva cópias de chaves privadas de titulares de certificados.

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

6.2.6. Inserção de chave privada em módulo criptográfico

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

6.2.7. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação das chaves privadas das AC Validar Múltipla é coordenada pela Supervisão de Serviços de AC, onde 2 de um grupo de 4 funcionários com perfis qualificados da AC Validar Múltipla, detentores de partição da chave de ativação do equipamento criptográfico (PIN), apresentam tais componentes em cerimônia específica.

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

6.2.9. Método de desativação de chave privada

A chave privativa da AC Validar Múltipla, instalada em ambiente de produção dos sistemas de certificação localiza-se em nível de segurança 4, onde só é permitido o acesso ao ambiente em

duplas devidamente autorizadas pelo sistema de controle de acesso da AC Validar Múltipla.

Dentro deste ambiente, somente funcionários qualificados do departamento de operações têm acesso ao sistema de certificação de produção, onde são executados os comandos de desativação do sistema, após a sua devida identificação e autorização feita através de mecanismos nativos do sistema operacional.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.10. Método de destruição de chave privada

A Supervisão de PKI da AC Validar Múltipla, de posse da chave privada original e suas cópias de segurança a serem destruídas, acompanhado do Gerente de Segurança e do representante legal da AC Validar Múltipla, titular do certificado, conduz cerimônia específica, em ambiente de nível 4 de segurança, para reinicialização das mídias de armazenamento das chaves privadas, não deixando informações remanescentes sensíveis nessas mídias

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

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da AC Validar Múltipla e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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

6.3.2.1. As chaves privadas dos titulares dos certificados de assinatura digital emitidos pela AC Validar Múltipla 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 Validar Múltipla 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 Validar Múltipla 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

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

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC Validar Múltipla são únicos e aleatórios.

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

6.4.2. Proteção dos dados de ativação.

6.4.2.1. A AC Validar Múltipla garante que os dados de ativação de sua chave privada 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 Validar Múltipla é realizada em ambiente próprio para a condução de Cerimônia de Geração de Chaves. O ambiente computacional é 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 Validar Múltipla são descritos em cada PC implementada.

6.5.1.3. O ambiente computacional da AC Validar Múltipla relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados,

implementa, entre outras, as seguintes funções:

a) controle de acesso aos serviços e perfis da AC Validar Múltipla;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Validar Múltipla;
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 Validar Múltipla;
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 mecanismos de segurança física.

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção deverá ter 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 Validar Múltipla, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC Validar Múltipla. Todos esses eventos deverão ser registrados para fins de auditoria.

6.5.1.6. Equipamentos utilizados pela AC Validar Múltipla são preparados e configurados como previsto na Política de Segurança da AC Validar Múltipla ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A segurança computacional da AC Validar Múltipla segue as recomendações *Common Criteria*.

6.5.3. Controle de segurança para as Autoridades de Registro

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

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

a) Controle de acesso lógico ao sistema operacional;
b) Exigência de uso de senhas fortes;
c) Diretivas de senha e de bloqueio de conta;
d) Logs de auditoria do sistema operacional ativados, registrando:

i. Iniciação e desligamento do sistema;
ii. Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
iii. Mudanças na configuração da estação;
iv. Tentativas de acesso (login) e de saída do sistema (logoff);
v. Tentativas não autorizadas de acesso aos arquivos de sistema;
vi. Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.

a) Antivírus, antitrojan e *antispyware*, instalados, atualizados e habilitados;
b) Firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;
c) Proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
d) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix etc.);
e) Utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
f) Impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
g) Utilização de data e hora de Fonte Confiável do Tempo (FCT).

6.5.3.3. Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1. A AC Validar Múltipla adota Sistema de Certificação Digital desenvolvido por terceiros. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente da AC Validar Múltipla avalia e decide quando será a implementação no ambiente de produção.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC Validar Múltipla provêm documentação suficiente para suportar avaliações externas de segurança dos seus componentes.

6.6.2. Controle de gerenciamento de segurança

6.6.2.1. A AC Validar Múltipla verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas

através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. Uma metodologia formal de gerenciamento de configuração é ser usada para a instalação e a contínua manutenção do sistema de certificação da AC Validar Múltipla.

6.6.3. Classificação 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 Validar Múltipla 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 Validar Múltipla, incluindo firewalls e recursos similares.

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

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

6.7.1.4. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (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 Validar Múltipla.

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

6.7.3. Sistema de detecção de intrusão (IDS)

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

6.7.3.2. O sistema de detecção de intrusão reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento.

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

6.7.4. Registro de acessos não-autorizados à rede

As tentativas de acesso não autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. Carimbo de Tempo

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. Perfil do Certificado

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

7.1.1. Número de versão

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

7.1.2. Extensões de certificado

Não se aplica.

7.1.3. Identificadores de algoritmo
Não se aplica.

7.1.4. Formatos de nome

7.1.4.1. Não se aplica.

7.1.5. Restrições de nome

Não se aplica.

7.1.6. OID (Object Identifier) da DPC

O OID desta DPC é 2.16.76.1.1.197.

7.1.7. Uso da extensão "*Policy Constraints*"

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Não se aplica.

7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC Validar Múltipla implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC Validar Múltipla e sua criticalidade.

7.2.2.2. As LCR da AC Validar Múltipla obedecem a ICP - Brasil que define como obrigatórias as

seguintes extensões de LCR

a) ***Authority Key Identifier***, não crítica: contém o hash SHA-1 da chave pública da AC Validar Múltipla;
b) ***CRL Number***, não crítica: contém um número sequencial para cada LCR emitida pela AC Validar Múltipla.

7.3. Perfil de OCSP

7.3.1. Número (s) de versão

Não se aplica.

7.3.2. Extensões de OCSP

Não se aplica.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. Frequência e circunstâncias das avaliações

A AC Validar Múltipla, entidade integrante da ICP-Brasil, sofreu auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento

8.2. Identificação / Qualificação do avaliador

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

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

8.3. Relação do avaliador com a entidade avaliada

As auditorias das entidades integrantes da ICP-Brasil são realizadas por empresas de auditoria independentes credenciadas pela AC Raiz, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.4. Tópicos cobertos pela avaliação

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

8.4.2. A AC Validar Múltipla 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 ICPBRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3. As entidades da ICP-Brasil diretamente vinculadas à AC Validar Múltipla (AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC Validar Múltipla é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

8.5. Ações tomadas como resultado de uma deficiência

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

8.6. Comunicação dos resultados

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

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

Variável conforme política Comercial da AC Validar Múltipla.

9.1.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

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

9.1.4. Tarifas para outros serviços

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

9.1.5. Política de reembolso

Não se aplica.

9.2. Responsabilidade Financeira

A responsabilidade da AC Validar Múltipla será verificada conforme previsto na legislação brasileira.

9.2.1. Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2. Outros ativos

Conforme regramento desta DPC.

9.2.3. Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3. Confidencialidade da informação do negócio

9.3.1. Escopo de informações confidenciais

9.3.1.1. Como regra geral, todos os documentos, informações ou registros fornecidos à AC ou às ARs são sigilosos.

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

9.3.2. Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas compreendem:

a) os certificados e a LCR emitidos pela AC Validar Múltipla;
b) Informações corporativas ou pessoais que façam parte de certificados ou em diretórios públicos;
c) as PCS implementadas pela AC;
d) esta DPC;
e) versões públicas da Política de Segurança; e
f) resultados finais de auditorias.

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

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

a) qualquer PC aplicável;
b) qualquer DPC;
c) versões públicas de Política de Segurança – PS; e
d) a conclusão dos relatórios de auditorias.

9.3.2.3. A AC Validar Múltipla também poderá divulgar, forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados emitidos no âmbito da ICP-Brasil. Responsabilidades em proteger a informação confidencial

9.3.3. Responsabilidade em proteger a informação confidencial

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

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

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

9.3.3.4. Não se aplica.

9.4. Privacidade da informação pessoal

9.4.1. Plano de privacidade

A AC Validar Múltipla assegurará a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2. Tratamento de informação como privadas

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

9.4.3. Informações não consideradas privadas

Informações sobre revogação de certificados de usuários finais são fornecidas na LCR da AC Validar Múltipla.

9.4.4. Responsabilidade para proteger a informação privadas

A AC Validar Múltipla e AR são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5. Aviso e consentimento para usar informações privadas

As informações privadas obtidas pela AC Validar Múltipla poderão ser utilizadas ou divulgadas a terceiros mediante expressas autorização do respectivo titular, conforme legislação aplicável.
O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

Autorizações formais podem ser apresentadas de duas formas:

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

9.4.6. Divulgação em processo judicial ou administrativo

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

As informações privadas ou confidenciais sob a guarda da AC Validar Múltipla poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da

autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7. Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8. Informações a terceiros

Como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC Validar Múltipla deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.5. Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

A AC Validar Múltipla declara e garante o quanto segue:

9.6.1.1. Autorização para certificado

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

9.6.1.2. Precisão da informação

A AC Validar Múltipla implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC Raiz, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das ARs na forma de suas DPCs, PCs e normas complementares.

9.6.1.3. Identificação do requerente

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

9.6.1.4. Consentimento dos titulares

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

9.6.1.5. Serviço

A AC Validar Múltipla mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios e LCRs.

9.6.1.6. Revogação

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

9.6.1.7. Existência Legal

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

9.6.2. Declarações e Garantias da AR

Em acordo com item 4 desta DPC.

9.6.3. Declarações e garantias do titular

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

9.6.3.2. A AC Validar Múltipla deve informar à AC SyngularID qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

9.6.4. Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes devem:

a) Recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
b) Verificar, a qualquer tempo, a validade do certificado.

9.6.4.2. O certificado da AC Validar Múltipla é considerado válido quando:

i. Tiver sido emitido pela AC;

ii. Não constar como revogado pela AC;
iii. Não estiver expirado; e
iv. Puder ser verificado com o uso do certificado válido da AC.

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

9.6.5. Representações e garantias de outros participantes

Não se aplica.

9.7. Isenção de garantias

Não se aplica.

9.8. Limitações de responsabilidades

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

9.9. Indenizações

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

9.10. Prazo e Rescisão

9.10.1. Prazo

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

9.10.2. Término

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

9.10.3. Efeito da rescisão e sobrevivência

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

9.11. Avisos individuais e comunicações com os participantes

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

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC Validar Múltipla mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web (http://syngularid.com.br/repositorio/ac-validar-multipla/dpc/dpc-ac-validar-multipla.pdf).

9.12.3. Circunstâncias na qual o OID deve ser alterado

Não se aplica.

9.13. Solução de conflitos

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

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

9.14. Lei aplicável

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

9.15. Conformidade com a Lei aplicável

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

9.16. Disposições Diversas

9.16.1. Acordo completo

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

9.16.2. Cessão

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

9.16.3. Independência de disposições

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

9.16.4. Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

10. DOCUMENTOS REFERENCIADOS

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

REF	NOME DO DOCUMENTO	CÓDIGO
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP- BRASIL	**DOC-ICP-06**

[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-09**
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-08**
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTODAS 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]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP BRASIL	**DOC-ICP-01.01**
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	**DOC-ICP-05.02**

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

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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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

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

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