Declaração de Práticas de Certificação

Autoridade Certificadora Digital Múltipla

OID: 2.16.76.1.1.166

Versão 2.0 de 30 de janeiro de 2023

Classificação: Pública

Sumário

Controle de Versões

Versão	Data	Descrição
1.0	01.02.2021	Versão inicial, a partir do DOC-ICP-05 versão 6.1.
1.1	04.06.2021	Adequação ao nome da AC.
2.0	30.01.2023	Atualização a partit do DOC-ICP-05 versão 6.3

1 INTRODUÇÃO

1.1 Visão Geral

1.1.1

Esta DPC estabelece as práticas e os procedimentos empregados pela Autoridade Certificadora DIGITAL MÚLTIPLA, integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC DIGITAL MÚLTIPLA na execução de seus serviços.

1.1.2

Esta DPC foi elaborada adotando a mesma estrutura empregada no DOC-ICP-05.

1.1.3

Não se aplica.

1.1.4

A estrutura desta DPC está baseada na RFC 3647.

1.1.5

A AC DIGITAL MÚLTIPLA mantém todas as informações desta 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 do documento e identificação

1.2.1

Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora DIGITAL MÚLTIPLA, e referida como “DPC AC DIGITAL MÚLTIPLA”, cujo Identificador de Objeto (OID) é 2.16.76.1.1.166.

1.2.2

A AC DIGITAL MÚLTIPLA emissora de certificados para usuários finais, é exclusiva e separada de acordo com o propósito de assinatura de documento e proteção de e-mail (S/MIME).

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

Esta DPC se refere exclusivamente à AC DIGITAL MÚLTIPLA, integrante da ICP-Brasil.

1.3.2 Autoridades de Registro

1.3.2.1 Na página web (url) http://repositorio.acdigital.com.br encontram-se publicados os dados a seguir,

referentes às Autoridades de Registro (ARs) utilizadas pela AC para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

a) relação de todas as ARs credenciadas; e
b) relação de ARs que tenham se descredenciado da cadeia da AC DIGITAL MÚLTIPLA, com respectiva data do descredenciamento.
c) não se aplica.

1.3.3 Titulares de Certificado

Podem ser titulares de certificados emitidos segundo esta DPC pessoas físicas e jurídicas.

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

A AC DIGITAL MÚLTIPLA publica em sua página Web (URL) - http://repositorio.acdigital.com.br/ - a relação de todos os Prestadores de Suporte – PSS, Prestadores de Serviços Biométricos – PSBIOs e Prestadores de Serviço de Confiança – PSC, vinculados a AC DIGITAL MÚLTIPLA, responsável por esta DPC.

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do Certificado

A AC DIGITAL MÚLTIPLA implementa as seguintes Políticas de Certificado Digital, para Certificados de Assinatura Digital:

a) PC A1 da AC DIGITAL Múltipla – OID: 2.16.76.1.2.1.108
b) PC A3 da AC DIGITAL Múltipla – OID: 2.16.76.1.2.3.103

1.4.2 Uso proibitivo do certificado

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

1.5 Política de Administração

1.5.1 Organização administrativa do documento

Autoridade Certificadora DIGITAL MÚLTIPLA.

1.5.2 Contatos

AC DIGITAL Múltipla

Endereço: Rua General Andrade Neves, 90, Sala 04, Centro, Porto Alegre – RS, CEP: 90.010-210

Telefone: +55 (51) 3025-7630

Pág. Web: www.acdigital.com.br
E-mail: normas@acdigital.com.br

1.5.3 Pessoa a quem determina a adequabilidade da DPC como a PC

A/C: Sidinei Gomes
Telefones: +55 (51) 3025-7630
E-mail: normas@acdigital.com.br

1.5.4 Procedimentos de aprovação da DPC

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

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM – SEI	Capability Maturity Model do Software Engineering Institute
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro de Pessoas Físicas

SIGLA	DESCRIÇÃO
CS	Code Signing
CSR	Certificate Signing Request
DETRAN	Departamento Nacional de Trânsito
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Instrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecummunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	On-line Certificate Status Protocol
OID	Object Identifer
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit

SIGLA	DESCRIÇÃO
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIN	Personal Identification Number
PIS	Programa de Integração Social
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
PUK	PIN Unbloking Key
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SIGEPE	Sistema de Gestão de Pessoal da Administração Pública Federal
SNMP	Simpe Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSL	Transport Layer Security
TSDM	Trusted Software Development Methodology
TSE	Tribunal Superior Eleitoral
UF	Unidade da Federação
URL	Uniform Resource Locator

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

2.1.1

A AC DIGITAL MÚLTIPLA mantém disponível repositório atendendo as seguintes obrigações:

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

2.1.2

Os requisitos aplicáveis ao repositório da AC DIGITAL MÚLTIPLA responsável por esta DPC, são:

a) localização física e lógica;
b) disponibilidade, a definida acima;
c) protocolos de acesso – HTTP e HTTPS com controles de acesso físico e lógico que impossibilitam a escrita ou a alteração dos dados por terceiros; e
d) requisito de segurança – só pessoas com autorização é que podem editar o repositório.

2.1.3

O repositório da AC DIGITAL MÚLTIPLA está disponível para consulta durante 24 (vinte e quatro) horas pordia, 7 (sete) dias por semana.

2.1.4

A AC DIGITAL MÚLTIPLA disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas para distribuição de sua LCR:

1. http://repositorio.acdigital.com.br/lcr/ac-digital-multipla-g1.crl
2. http://repositorio2.acdigital.com.br/lcr/ac-digital-multipla-g1.crl

2.2 Publicação de informações dos certificados

2.2.1

A AC DIGITAL MÚLTIPLA mantém disponível em sua página *web* as informações descritas no item 2.2.2 no endereço *http://repositorio.acdigital.com.br/*. A disponibilidade da página é de no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2

As seguintes informações são publicadas na página web **http://repositorio.acdigital.com.br/**:

a) seu próprio certificado;
b) suas LCR's;
c) sua DPC;
d) as PC's que implementa;

e) uma relação atualizada, contendo as ARs vinculadas e seus respectivos endereços;
f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3 Tempo ou Frequência de Publicação

As informações mencionadas no item anterior serão publicadas sempre que sofrerem alterações, após aprovação da entidade competente, quando necessário.

As LCRs da AC DIGITAL MÚLTIPLA possuem uma frequência de emissão de 6 (seis) horas, podendo ser antecipada a sua emissão, as informações são publicadas imediatamente após sua emissão pela AC DIGITAL MÚLTIPLA.

2.4 Controle de Acesso aos Repositórios

A AC DIGITAL MÚLTIPLA não implementa restrições de acesso à leitura desta DPC, PC's e LCR's emitidas por ela.

Os acessos para escrita estão restritos às pessoas responsáveis previamente designadas para o cargo/função.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Atribuição de Nomes

3.1.1 Tipos de nomes

3.1.1.1 Os tipos de nomes admitidos para os titulares de certificados da AC DIGITAL MÚLTIPLA, segundo esta DPC é o "Distinguished Name" (DN), no padrão ITU X.500:

1. Certificados de pessoa física
   a) o campo "Common Name" (CN) é composto do nome do titular do certificado.
2. Certificados de pessoa jurídica:
   a) o campo "Common Name" (CN) é composto do nome empresarial de pessoa jurídica.

3.1.1.2 Não se aplica.

3.1.2 Necessidade de nomes significativos

Os certificados emitidos pela AC DIGITAL MÚLTIPLA fazem uso de nomes significativos que possibilitam determinar de forma inequívoca a identidade da pessoa ou organização a que se referem, para identificação dos titulares de 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

Identificadores "*Distinguished Name*" (DN) são únicos para titulares de certificado da AC DIGITAL MÚLTIPLA.

Números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo. A AC DIGITAL MÚLTIPLA utiliza a nomenclatura do CPF para certificados de pessoa física e o CNPJ para certificados de pessoa jurídica para garantir a unicidade dos nomes.

3.1.6 Procedimento para resolver disputa de nomes

A AC DIGITAL MÚLTIPLA reserva-se o direito de tomar todas as decisões referentes as disputas decorrentes da igualdade de nomes de titular de certificado. Durante o processo de confirmação de identidade, o solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

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

A AC DIGITAL MÚLTIPLA reserva-se ao direito de revogar qualquer certificado envolvido em uma disputa.

3.2 Validação inicial de identidade

Neste item e nos seguintes, esta DPC descreve em detalhes os requisitos e procedimentos utilizados pelas ARs vinculadas à AC DIGITAL MÚLTIPLA para 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, observado o quanto segue:
   i. para certificados de pessoa física: comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim.
   ii. para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado, e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.

b) emissão do certificado: 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

O sistema de certificação utilizado pela AC DIGITAL MÚLTIPLA e suas ARs no gerenciamento do ciclo de vida dos certificados, garante a entrega somente ao detentor da chave privada correspondente à chave pública constante do certificado.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida na solicitação. Ao recebê-la o software utilizado pela AC DIGITAL MÚLTIPLA procede a verificação automática da assinatura digital com uso da chave pública incluída nessa solicitação.

Todo o processo de geração da solicitação de certificado (CSR PKCS#10), emissão de certificado e ativação de certificado do titular é realizada de forma automática com registro dos passos realizados, referenciando o descrito no RFC 4210 e RFC 6712.

3.2.2 Autenticação da identificação da organização

3.2.2.1 Disposições Gerais

3.2.2.1.1 Os procedimentos empregados pelas ARs vinculadas para a confirmação da identidade de uma pessoa jurídica são feitos mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos, ou por videoconferência mediante regras previamente estabelecidas pela AC Raiz por instrução normativa.

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 da pessoa física, 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 a 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 administradores, quando aplicável;

b) Relativos à sua habilitação fiscal:
   i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
   ii. prova de inscrição no Cadastro Específico do INSS – CEI.

NOTA 1: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desdeque 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 CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[1];

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);[2]

c) nome completo do responsável pelo certificado, sem abreviações;[3] e

d) data de nascimento do responsável pelo certificado.[4]

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 devrá ser realizada mediante a presença física do interessado ou por um dos procedimentos listados abaixo, que 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 e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico:

a) por módulo de AR eletrônico, exclusivamente nos casos previstos no regulamento;

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 Procedimentos para identificação de um indivíduo

A identificação da pessoa física requerente do certificado deverá ser realizada como se 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 regulamento 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 ou 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.

NOTA 2: Em caso de documento pouco legíveis ou danificado, a AC DIGITAL MÚLTIPLA, reserva-se ao direito de solicitar mais do que um documento de identificação.

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, serão verificados:

a) por agente de registro distinto do que realizou a etapa de identificação;
b) pela AR ou AR própria da AC ou ainda AR própria do PSS da AC DIGITAL MÚLTIPLA; 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

3.2.3.2 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; [5]

b) data de nascimento. [6]

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) Cadastro de Pessoa Física (CPF);

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

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

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

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

f) 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.

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.

---

1. No campo Subject Alternative Name, OID 2.16.76.1.3.2.3
2. No campo Subject Alternative Name, OID 2.16.76.1.3.2 4
3. No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.4

5 No campo Subject, como parte do Common Name, que compõe o Distinguished Name

6 No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.1

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 um 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

3.2.7.6 Não se aplica.

3.2.7.7 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.

3.2.7.8 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.

3.2.7.9 Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

3.2.7.10 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 DIGITAL MÚLTIPLA mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC DIGITAL 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, 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 exigea 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.

3.2.8.3 Será mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.1 Não se aplica.

3.2.8.3.2 Não se aplica.

3.2.8.4 A AC DIGITAL 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 documento CRÍTERIOS E PROCEDIMEENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6] e em regulamento editado por instrução normativa da AC Raiz que define os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil.

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.

3.2.9 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

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

O processo de geração pela AC DIGITAL MÚLTIPLA de um novo certificado para um titular de certificado, pode ser feito de forma simplificada, antes da expiração da validade do certificado.

A AC DIGITAL MÚLTIPLA comunica o titular de certificado, por e-mail, ou por meios equivalentes, da necessidade de renovação do certificado, com antecedência mínima de 30 (trinta) dias.

3.3.2 Esse processo poderá ser conduzido por uma das seguintes possibilidades:

O 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 válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;

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

representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;

d) solicitação por meio eletrônico dada nas alíneas 'b' e 'c', acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação a ser editada pela AC Raiz ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;

e) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar um nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométrica, 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

Caso sejam requeridos procedimentos específicos para as PC implementadas, os mesmos devem ser descritos nessas PC, no item correspondente.

3.3.4

Não se aplica.

3.4 Identificação e Autenticação para solicitação de revogação

O solicitante da revogação de certificado deverá ser identificado. O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3. Solicitações de revogação de certificados devem ser registradas.

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 Solicitação do certificado

Os requisitos e procedimentos operacionais estabelecidos pela AC DIGITAL MÚLTIPLA e ARs vinculadas para a solicitação de emissão de certificado são:

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 certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico.

Nota 1: na impossibilidade técnica de assinatura digital do termo de titularidade será aceita a assinatura

manuscrita do termo ou assinatura digital do termo com o uso do certificado ICP-Brasil do titular do certificado ou responsável pelo uso do 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 de solicitação deve ser sempre por intermédio da AR.

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

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

4.1.2.1 Responsabilidades da AC

4.1.2.1.1 A AC DIGITAL MÚLTIPLA responde pelos danos a que der causa.

4.1.2.1.2 A AC DIGITAL 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

São obrigações da AC DIGITAL MÚLTIPLA, responsável por esta DPC:

a) operar de acordo com DPC da AC DIGITAL MÚLTIPLA e com as PCs que implementa;
b) gerar e gerenciar os seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de usuários finais;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCRs;
k) publicar em sua página *web* a 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 sua 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) implementadas, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

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

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

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

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

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

v) informar à AC Raiz 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 AC que utilize seus serviços; e

y) garantir que todas as aprovações de solicitação de certificado sejam realizadas por agente de registro e estação de trabalho autorizados.

4.1.2.3 Responsabilidades da AR

A AR será responsável pelos danos que der causa.

4.1.2.4 Obrigações das ARs

As obrigações das ARs vinculadas à AC DIGITAL 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 da AC DIGITAL MÚLTIPLA, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC responsável utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que define as características mínimas de segurança para as AR da ICP-Brasil;

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, critério, práticas e regras estabelecidas pela AC DIGITAL MÚLTIPLA e pela ICP-Brasil, em especial com o contido em regulamento editado por instrução normativa da AC Raiz que define as características mínimas de segurança para as AR da ICP-Brasil, 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 DIGITAL MÚLTIPLA e suas ARs vinculadas 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 DIGITAL MÚLTIPLA e suas ARs vinculadas 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 DIGITAL 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 DIGITAL Múltipla durante a emissão de um certificado

4.3.1.1 A emissão de um certificado pela AC DIGITAL MÚLTIPLA é realizado através de uma validação do preenchimento de formulário da solicitação de certificado, bem como a documentação obrigatória a ser apresentada no momento da validação inicial.

O AGR e titular de certificado assinam o documento TERMO DE TITULARIDADE [4], de forma a garantir que as informações contidas se encontram corretas e são verídicas, o AGR através do sistema disponibilizado pela AC DIGITAL MÚLTIPLA, aprova a solicitação de certificado que será enviado para verificação, ou em casos de consulta automática é aprovado sem a necessidade de um verificador.

É disponibilizado ao titular de certificado a possibilidade de emissão após a correta aprovação. O titular do certificado é notificado da emissão por e-mail ou equivalente.

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

4.3.2 Notificação para o titular do certificado pela AC na emissão do certificado

O sistema da AC DIGITAL MÚLTIPLA emite uma notificação via e-mail ou equivalente, informando o titular do certificado sobre a sua emissão.

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado

4.4.1.1 A aceitação de certificado pelo titular é realizada pela conferência das informações contidas no certificado. Caso as informações estejam divergentes o titular de certificado deverá solicitar imediatamente a revogação do referido certificado.

Ao aceitar o certificado o titular de certificado:

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

4.4.1.2 A aceitação de todo certificado emitido é declarado pelo respectivo titular. No caso de certificados de pessoas jurídicas, a aceitação é feita pela pessoa física responsável pelo uso subsequente ao recebimento do certificado.

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

4.4.2 Publicação do certificado pela AC

O certificado da AC DIGITAL 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

A notificação se dará de acordo com item 2.2 da DPC da AC Raiz.

4.5 Usabilidade da Chave privada e do certificado do titular

A AC DIGITAL MÚLTIPLA opera de acordo com a sua própria Declaração de Práticas de Certificação – DPCe com as Políticas de Certificado – PC que implementar, estabelecidos em conformidade com os documentos REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1 Usabilidade da Chave privada e de certificado do titular

4.5.1.1 O titular 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 do titular de certificado emitido de acordo com esta DPC AC DIGITAL MÚLTIPLA são as abaixo relacionadas:

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

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 o item 3.3 desta DPC.

4.6.2 Quem pode solicitar a renovação

Em acordo com o item 3.3 desta DPC.

4.6.3 Processamento de requisição para renovação de certificados

Em acordo com o item 3.3 desta DPC.

4.6.4 Notificação para nova emissão de certificado para o titular

Em acordo com o item 3.3 desta DPC.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com o 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 o 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 Um certificado emitido pela AC DIGITAL MÚLTIPLA pode ser revogado a qualquer instante, pelo titular do certificado, pela AC DIGITAL MÚLTIPLA no caso de suspeita de fraude ou por decisão motivada da AC Raiz, resguardados os princípios do contraditório e da ampla defesa.

4.9.1.2 Um 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 DPC DIGITAL MÚLTIPLA observa ainda que:

a) A AC DIGITAL Múltipla revogará, no prazo definido no item 4.9.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil; e
b) O CG da ICP-Brasil ou a AC Raiz determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP- Brasil.

4.9.1.4 A AC DIGITAL MÚLTIPLA verifica a validade do certificado, 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 confirmada por meio das verificações da assinatura da AC DIGITAL MÚLTIPLA e do período de validade da LCR.

4.9.2 Quem pode solicitar revogação

Esta DPC estabelece que para 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 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 DIGITAL MÚLTIPLA;
e) por uma AR vinculada;
f) por determinação da AC DIGITAL MAIS, 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 O titular pelo certificado pode solicitar a revogação de certificado emitido pela AC DIGITAL MÚLTIPLA através de formulário específico para o caso, devidamente preenchido e assinado pelo representante legal.

Os meios necessários para se proceder à revogação do certificado estão disponíveis a qualquer tempo para os agentes habilitados conforme item 4.9.2.

4.9.3.2 Fica estabelecido como diretrizes gerais que:

a) o solicitante da revogação de um certificado deve ser identificado;
b) as solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e

armazenadas;

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

d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.9.3.3 O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 24 (vinte e quatro) horas.

4.9.3.4 Não se aplica.

4.9.3.5 A AC DIGITAL 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 correspondente LCR.

4.9.3.6 Não se aplica.

4.9.4 Prazo para solicitação de revogação

4.9.4.1 A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 desta DPC. A AC DIGITAL MÚLTIPLA estabelece o prazo de 7 (sete) dias para a aceitação do certificado solicitado por seu titular, dentro dos quais a revogação do certificado poderá ser solicitado sem cobrança de tarifa pela AC DIGITAL MÚLTIPLA.

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 DIGITAL MÚLTIPLA processa a revogação de forma imediata após a análise do pedido.

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

Não se aplica.

4.9.7 Frequência de emissão de LCR

4.9.7.1 A AC DIGITAL MÚLTIPLA emite uma nova LCR referente a certificados de usuários finais a cada 6 (seis) horas, podendo emitir a sua LCR por períodos inferiores ao estabelecido.

4.9.7.2 A frequência máxima admitida para a emissão de LCR para os certificados de usuário finais é de 6 (seis) 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 AC DIGITAL MÚLTIPLA publica sua LCR em seu repositório em no máximo 4 (quatro) horas após a sua geração.

4.9.9 Disponibilidade para revogação/verificação de status on-line

O processo de revogação *on-line* está disponível no sistema de certificação da AC DIGITAL MÚLTIPLA como em página *web* disponibilizada pela AC DIGITAL MÚLTIPLA.

A AC DIGITAL MÚLTIPLA suporta verificação *on-line* de status de certificados, através de consulta da sua CRL (*Certificate Revocation List*).

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 Quando houver comprometimento ou suspeita de comprometimento da chave privada, o Titular do Certificado deverá comunicar imediatamente à AC DIGITAL MÚLTIPLA.

4.9.12.2 A comunicação à AC DIGITAL MÚLTIPLA deverá ser através dos dados de contato informados no item 1.5.2, ou através de formulário de solicitação de revogação de forma presencial na AR.

4.9.13 Circunstâncias para suspensão

Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados da AC DIGITAL MÚLTIPLA.

4.9.14 Quem pode solicitar suspensão

A AC, aprovados 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 DIGITAL 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

Sendo necessária a extinção dos serviços da AC DIGITAL MÚLTIPLA, AR, PSS ou PSBio vinculado, a AC DIGITAL MÚLTIPLA irá executar os procedimentos aplicáveis descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.11.2

Os procedimentos e requisitos de são adotados, nos casos de extinção ou encerramento dos serviços da AC DIGITAL MÚLTIPLA, de uma AR, PSS ou PSBio a ela vinculado, são:

a) notificar a AC Raiz;
b) extinção dos serviços de emissão de certificados finais;
c) notificar o titular do certificado;
d) publicação pública sobre a extinção dos serviços da AC DIGITAL Múltipla;
e) transferência progressiva de seus serviços operacionais para um sucessor que possua os mesmos requisitos de segurança;
f) transferência progressiva de seus dados não críticos para um sucessor com os mesmos requisitos de segurança;
g) transferência segura de seus dados críticos para um sucessor com os mesmos requisitos de segurança.

Nos casos em que haja mais do que um sucessor envolvido na obtenção dos dados da AC DIGITAL MÚLTIPLA, esta por sua vez solicitará um parecer à AC Raiz.

Nos casos de extinção falência ou encerramento de AR vinculadas à AC DIGITAL MÚLTIPLA, devendo seguir os mesmos procedimentos que a AC DIGITAL MÚLTIPLA, em caso de disputa por arquivamento da informação da AR a AC DIGITAL MÚLTIPLA assumirá o arquivamento dos dados.

4.12 Custódia e recuperação de chave

4.12.1 Política e práticas de custódia e recuperação de chave

A AC DIGITAL MÚLTIPLA não implementa a recuperação (*escrow*) de chaves privadas, isto é, não permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

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

A AC DIGITAL MÚLTIPLA não executa tais práticas.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes estão descritos os controles de segurança implementados pela AC DIGITAL MÚLTIPLA, responsável pela DPC e pelas ARs a ela vinculadas, para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 Controles Físicos

Nos itens seguintes da DPC da AC DIGITAL MÚLTIPLA, encontra-se descrito os controles físicos referentes às instalações que abrigam os sistemas da AC DIGITAL MÚLTIPLA e instalações das ARs vinculadas.

5.1.1 Construção e localização das instalações de AC

5.1.1.1 A localização e o sistema de certificação utilizado para a operação da AC DIGITAL MÚLTIPLA não são publicamente identificados, nem há identificação pública externa das instalações. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2 Todos os aspectos de construção das instalações da AC DIGITAL MÚLTIPLA, relevantes para os controles de segurança física, foram executadas por técnicos especializados e compreendem, entre outros, os descritos abaixo:

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

5.1.2 Acesso físico

O acesso físico às dependências da AC DIGITAL MÚLTIPLA, onde são realizadas as atividades relacionadas aos processos de gerenciamento de certificados da AC DIGITAL MÚLTIPLA é gerenciado e controlado internamente de acordo com os requisitos definidos na POLÍTICA DE SEGURANÇA DA ICP- BRASIL [8] e os requisitos que seguem.

5.1.2.1 Níveis de Acesso

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

5.1.2.1.2 O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC DIGITAL 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 DIGITAL MÚLTIPLA transitam apenas devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC DIGITAL MÚLTIPLA é executado nesse nível.

5.1.2.1.3 Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC DIGITAL MÚLTIPLA, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4 O segundo nível – ou nível 2 – é interno ao primeiro nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC DIGITAL 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 – é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por, pelo menos, um funcionário que tenha esta permissão.

5.1.2.1.6 No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual, com 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, não são admitidos a partir do nível 3.

5.1.2.1.8 O quarto nível – ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da AC DIGITAL 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 os sistemas das suas ARs vinculadas. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

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

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

5.1.2.1.11 A AC DIGITAL MÚLTIPLA possui dois ambientes de nível 4, um referente ao ambiente de produção e um outro para o ambiente de backup ou contingência. Ambos os sites possuem:

a) equipamentos de produção on-line e cofre 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 – ou nível 5 – é interno aos ambientes de nível 4 e compreende o cofre. 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 ou o gabinete obedecem às seguintes especificações mínimas:

a) é feito em aço ou material de resistência equivalente; e
b) possui tranca com chave.

5.1.2.1.14 O sexto nível – ou nível 6 – consiste em pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da AC DIGITAL MÚLTIPLA estão armazenados em um 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 câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2 As fitas de vídeo resultantes da gravação 24x7 são armazenadas por 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3 Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes.

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

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

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

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 implementados pela AC DIGITAL 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 DIGITAL MÚLTIPLA é dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC DIGITAL MÚLTIPLA e seus respectivos serviços. Há um sistema de aterramento implantado.

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

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

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

5.1.3.5 São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL [7]. Qualquer modificação na rede é previamente documentada.

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

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

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

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

5.1.3.10 A capacidade de redundância de toda a estrutura de energia e ar-condicionado da AC DIGITAL 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 das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2 Nas instalações da AC DIGITAL MÚLTIPLA não é permitido fumar ou portar objetos que produzam fogo, ou faísca.

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

5.1.5.4 Em caso de incêndio nas instalações da AC DIGITAL MÚLTIPLA, a temperatura interna da sala cofre não

excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, 1 (uma) hora.

5.1.6 Armazenamento de mídia

A AC DIGITAL 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*) para AC DIGITAL MÚLTIPLA

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

5.2 Controles Procedimentais

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

5.2.1 Perfis qualificados

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

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

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

5.2.1.3.1 Não se aplica.

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

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1 Controle multiusuário é requerido para a geração e a utilização da chave privada da AC DIGITAL 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 DIGITAL MÚLTIPLA necessitam da presença de no mínimo 2 (dois) empregados da AC DIGITAL MÚLTIPLA com perfis qualificados. As demais tarefas da AC DIGITAL 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 DIGITAL MÚLTIPLA terá sua identidade e perfil verificados antes de:

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

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

a) ser diretamente atribuídos a um único empregado da AC DIGITAL MÚLTIPLA devidamente qualificado;
b) não compartilhados; e
c) ser restritos às ações associadas ao perfil para o qual foram criados.

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

5.2.4 Funções que requerem separação de deveres

A AC DIGITAL Múltipla impõe a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3 Controles de Pessoal

A AC DIGITAL MÚLTIPLA implementa procedimentos e requisitos, pelas ARs e PSS vinculados em relação a todo o seu pessoal, referente a aspectos como:

a) verificação de antecedentes e de idoneidade;
b) treinamento e reciclagem profissional;
c) sanções por ações não autorizadas; e
d) controles para contratação e documentação a ser fornecida.

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

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

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC DIGITAL MÚLTIPLA e AR vinculada envolvido em atividades diretamente relacionadas com o ciclo de vida dos certificados é admitido conforme o estabelecido na Política de Segurança da AC DIGITAL MÚLTIPLA e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC DIGITAL
MÚLTIPLA pode definir requisitos adicionais para a admissão.

5.3.2 Procedimentos de Verificação de Antecedentes

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

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

5.3.2.2 A AC DIGITAL MÚLTIPLA poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

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

a) Princípios e mecanismos de segurança da AC DIGITAL MÚLTIPLA e das AR vinculadas;
b) Sistema de certificação em uso na AC DIGITAL 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

Todo o pessoal da AC DIGITAL MÚLTIPLA e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC DIGITAL MÚLTIPLA ou das ARs.

5.3.5 Frequência e sequência de rodízios de cargos

A AC DIGITAL Múltipla não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC DIGITAL MÚLTIPLA ou de uma AR vinculada, A AC DIGITAL MÚLTIPLA suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação, irá instaurar processo administrativo para apurar

os fatos e, se for o caso, adotará as medidas legais cabíveis.

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

a) relato da ocorrência com "*modus operandis*";
b) identificação dos envolvidos;
c) eventuais prejuízos causados;
d) punições aplicadas, se for o caso; e
e) conclusões.

5.3.6.3 Concluído o processo administrativo, a AC DIGITAL MÚLTIPLA encaminha suas conclusões à ACRaiz.

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 DIGITAL MÚLTIPLA e das ARs vinculadas, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC DIGITAL MÚLTIPLA poderá definir requisitos adicionais para a contratação.

5.3.8 Documentação fornecida ao pessoal

5.3.8.1 A AC DIGITAL MÚLTIPLA disponibiliza para todo o seu pessoal e para as ARs vinculadas:

a) sua DPC;
b) as PCs que implementa;
c) POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
d) a Política de Segurança da AC DIGITAL MÚLTIPLA;
e) Documentação operacional relativa às suas atividades; e
f) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2 Toda a documentação fornecida ao pessoal é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC DIGITAL MÚLTIPLA e deverá ser mantida atualizada.

5.4 Procedimentos de Log de Auditoria

Nos itens seguintes estão descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC DIGITAL MÚLTIPLA, com o objetivo de manter um ambiente seguro.

5.4.1 Tipos de Evento Registrados

5.4.1.1 É registrado em arquivos de auditoria todos os eventos relacionados à segurança do sistema de certificação da AC DIGITAL MÚLTIPLA. Entre outros, os seguintes eventos estão obrigatoriamente incluídos em arquivos de auditoria.

a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC DIGITAL MÚLTIPLA;
c) mudanças na configuração da AC DIGITAL 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 de sistema;
g) geração de chaves próprias da AC DIGITAL MÚLTIPLA ou de chaves de Titulares de Certificados;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável;e
l) operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1 Não se aplica.

5.4.1.2 A AC DIGITAL MÚLTIPLA responsável por esta DPC, 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 DIGITAL MÚLTIPLA são todas as descritas nos itens acima.

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

5.4.1.5 Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC DIGITAL MÚLTIPLA é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA **I10CP**-BRASIL [8].

5.4.1.6 A AC DIGITAL MÚLTIPLA registrará eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos deverão obrigatoriamente estar 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.

5.4.1.7 A AC DIGITAL MÚLTIPLA que esteja vinculada a AR, define que o local de arquivamento dos dossiês dos

titulares serão armazenados em ambiente computacional da AC DIGITAL MÚLTIPLA, encontrando-se disponível para auditorias de conformidade.

5.4.2 Frequência de auditoria de registros

Os registros de auditoria da AC DIGITAL MÚLTIPLA serão analisados semanalmente pelo pessoal operacional da AC DIGITAL MÚLTIPLA com perfil adequado. Todos os eventos significativos serão explicados em relatório de auditoria de registros. Tal análise envolverá uma inspeção breve de todos os registros, verificando-se que não foram alterados, em seguida proceder-se-á a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise serão documentadas.

5.4.3 Período de Retenção para registros de Auditoria

A AC DIGITAL MÚLTIPLA manterá localmente os seus registros de auditoria pelo prazo mínimo de 2 (dois) meses e, subsequentemente, fará o armazenamento da maneira descrita no item 5.5.

5.4.4 Proteção de registro de Auditoria

5.4.4.1 O sistema de registros da AC DIGITAL MÚLTIPLA possui mecanismos, que visam a proteção dos seus registros de eventos contra leitura não autorizada, modificação e remoção.

5.4.4.2 Os registros de eventos são protegidos para evitar alterações e detectar adulteração, recorrendo a funções de hash, e para garantir que apenas pessoas com acesso autorizado possam realizar operações, sem modificar a integridade, autenticidade e confidencialidade dos dados, se necessário.

5.4.4.3 Os mecanismos de proteção descritos neste item obedecem à 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 do sistema de gerenciamento de certificados, plataformas criptográficas e demais componentes de infraestrutura, utilizados pela AC DIGITAL MÚLTIPLA, possuem cópias de segurança semanais, mensais e anuais, ou sempre que houver uma utilização dos equipamentos em ambiente *off-line*.

Os registros de auditoria são armazenados em local lógico dentro no mesmo nível em que operam os sistemas da AC DIGITAL MÚLTIPLA, com vista à proteção dos dados contra incêndio, sob o controle de pessoas autorizadas e em locais diferentes.

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

O sistema de coleta de dados de auditoria da AC DIGITAL MÚLTIPLA é uma combinação de processos automatizados e manuais, executada por seus sistemas ou por seu pessoal autorizado com perfil de execução.

5.4.7 Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC DIGITAL MÚLTIPLA não serão notificados à pessoa, organização, dispositivo ou aplicação que causou o evento; eventos que são considerados como possíveis problemas de violação de segurança, envolvendo o ciclo de vida do certificado, são escalados para a equipe de segurança de forma a serem avaliados e tratados.

5.4.8 Avaliações de vulnerabilidade

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

5.5 Arquivamento de Registros

Nos seguintes itens desta DPC é descrita a Política Geral de Arquivamento de Registros, para uso futuro, implementada pela AC DIGITAL MÚLTIPLA e pelas suas ARs vinculadas.

5.5.1 Tipos de registros arquivados

A AC DIGITAL MÚLTIPLA registra e arquiva as seguintes informações a respeito de:

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 DIGITAL MÚLTIPLA; e
g) informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são (de):

a) as LCR referentes a certificados de assinatura digital, são retidos de forma permanente para fins de consulta histórica;
b) dossiês dos titulares ficam retidos, no mínimo, por 7 (sete) anos, a contar da data de expiraçãoou revogação do certificado; e
c) as demais informações, inclusive arquivos de auditoria, são retidas por um período mínimo de 7(sete) anos.

5.5.3 Proteção de arquivos

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

5.5.4 Procedimentos para cópia de arquivo

5.5.4.1 Uma segunda cópia de todo o material arquivado deverá ser armazenada em local externo à AC DIGITAL 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 DIGITAL MÚLTIPLA realiza a verificação da integridade dessas cópias de segurança, periodicamente a cada 6 (seis) meses.

5.5.5 Requisitos para datação de registros

Informações de data e hora dos registros baseiam-se na sincronização com a hora UTC (Coordinated Universal Time) fornecida pela AC Raiz. O formato de hora obedece ao formato YYYYMMDDHHMMSSZ, incluindo segundos mesmo que o número de segundos seja zero.

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

Todo o sistema de coleta de dados de arquivos utilizado pela AC DIGITAL MÚLTIPLA em seus procedimentos operacionais são internos. O sistema de coleta de dados atende aos requisitos de segurança deste item 5.

5.5.7 Procedimentos para obter e verificar informação de arquivo

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

Somente equipamentos e pessoas autorizados da AC DIGITAL MÚLTIPLA, pessoas com perfis adequado e confiáveis estão autorizadas a ter acesso aos arquivos.

5.6 Troca de chave

5.6.1

A AC DIGITAL MÚLTIPLA informa com 30 (trinta) dias de antecedência antes da expiração do certificado de usuário final, via e-mail cadastrado na emissão do certificado ou equivalente.

O titular de certificado pode a seu gosto realizar a renovação de seu certificado através do preenchimento de um formulário para o efeito, disponível pela AR, onde é encaminhado o processo do fornecimento do novo certificado.

5.6.2

Não se aplica.

5.7 Comprometimento e Recuperação de Desastre

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

5.7.1 Procedimentos gerenciamento de incidente e comprometimento

5.7.1.1 A AC DIGITAL MÚLTIPLA possui um Plano de Continuidade de Negócios – PCN, de acesso restrito, testado pelo menos uma vez por ano, garantindo assim a continuidade dos seus serviços cítricos. A AC DIGITAL MÚLTIPLA possui também um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

5.7.1.2 Os procedimentos no PCN das ARs vinculadas para recuperação, total ou parcial das atividadesdas ARs, contendo no mínimo as seguintes informações:

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo, falha de equipamentos, inundações e incêndios;
b) identificação e concordância de todas as responsabilidades e procedimentos de emergência;
c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários.

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

A AC DIGITAL MÚLTIPLA mantém site de contingência em local geograficamente separado que espelha sua instalação principal para que, caso recursos computacionais, software ou dados sejam corrompidos ou houver suspeita de corrupção, possa ser restaurada, utilizando conexões seguras e cifradas. Cópias de segurança de todos os softwares e dados são realizadas de forma regular. A AC DIGITAL MÚLTIPLA prioriza o restabelecimento de sua operação, dando prioridade na emissão de suas LCRs.

5.7.3 Procedimento no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado de entidade é revogado

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

a) todos os usuários que receberam um certificado são notificados o mais rapidamente possível;
b) notificar a AC Raiz do status do certificado da AC DIGITAL MÚLTIPLA;
c) A AC DIGITAL MÚLTIPLA solicita um novo certificado à AC Raiz:
d) geração de novos certificados de usuários.

5.7.3.2 Chave de entidade é comprometida

A AC DIGITAL MÚLTIPLA possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de comprometimento de sua chave privada. Após a identificação da causa, serão tomadas todas as providências para ativar o site de contingência.

5.7.4 Capacidade de continuidade de negócio após desastre

A AC DIGITAL MÚLTIPLA possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza.

Todos os esforços em caso de desastre natural serão em preservar a informação do site de produção e migrar a operação para o site de contingência.

5.8 Extinção da AC

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

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes estão definidas as medidas de segurança implementadas pela AC DIGITAL MÚLTIPLA, para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. São definidos também outros controles técnicos de segurança utilizados pela AC DIGITAL 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 A geração do par de chaves da AC DIGITAL MÚLTIPLA é realizada pela própria AC DIGITAL MÚLTIPLA, em módulo criptográfico que implementa as características de segurança estabelecidas pela ICP-Brasil, após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2 Os pares de chaves de entidade solicitante de certificado são gerados pelo próprio titular de certificado, em módulo criptográfico para proteger suas chaves criptográficas e os seus dados de ativação, após aprovação de emissão de seu pedido de certificado.

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

6.1.1.4 O processo de geração do par de chaves da AC DIGITAL MÚLTIPLA é feito por hardware específico com o padrão FIPS (*Federal Information Processing Standards*) 140-2, nível 3.

6.1.1.5 Cada PC implementada pela AC DIGITAL MÚLTIPLA define 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 A chave privada da AC DIGITAL MÚLTIPLA é gerada, armazenada e utilizada apenas em hardware criptográfico homologado na ICP-Brasil. O acesso a esse hardware é controlado por meio de chave criptográfica de ativação, de acordo com o definido em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

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 A AC DIGITAL MÚLTIPLA entregará à AC DIGITAL MAIS cópia de sua chave pública encarregada da emissão de seu certificado.

6.1.3.2 Chaves públicas de AC estão disponíveis para consulta em página web e serão entregues ao emissor de certificado por meio de uma troca on-line utilizando funções automáticas do software de certificação da AC DIGITAL MÚLTIPLA.

6.1.4 Entrega de chave pública da AC DIGITAL MÚLTIPLA às terceiras partes

As formas para a disponibilização do certificado da AC DIGITAL MÚLTIPLA, e de todos os certificados da cadeia de certificação, para os usuários da AC DIGITAL MÚLTIPLA e terceiras partes, compreendem:

a) no momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL

b) diretório;
c) página *web* da AC DIGITAL MÚLTIPLA; e
d) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1 O tamanho de chaves criptográficas associadas aos certificados emitido pela AC DIGITAL MÚLTIPLA estão definidos nas PCs que a AC DIGITAL MÚLTIPLA implementa. Os algoritmos e os tamanhos de chaves criptográficas utilizadas estão de acordo 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 da AC DIGITAL MÚLTIPLA seguem o padrão de Homologação da ICP-Brasil, conforme definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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.

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

6.1.7.1 As chaves privadas dos titulares de certificados emitidos pela AC DIGITAL MÚLTIPLA podem ser utilizadas para Assinatura Digital conforme especificado na PCs que implementa, nelas também estão as possíveis restrições.

6.1.7.2 A chave privada da AC DIGITAL 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 chave privada da AC DIGITAL MÚLTIPLA é gerada, armazenada e utilizada no mesmo componente criptográfico utilizado para a sua geração, homologado junto ao ITI. O acesso a esse hardware é controlado por meio de chave criptográfica de ativação.

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1 O módulo criptográfico de geração de chaves assimétricas da AC DIGITAL MÚLTIPLA utiliza hardware criptográfico, e adota o padrão que está definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.1.2 Os módulos de geração de chaves criptográficas dos Titulares de Certificados são aqueles definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil – requeridos para os módulos de geração de chaves criptográficos dos titulares de certificado. Cada PC implementada especifica os requisitos adicionais aplicáveis.

6.2.2 Controle “n de m” para chave privada

6.2.2.1 A AC DIGITAL MÚLTIPLA implementa o controle múltiplo para a ativação e desativação da sua chave privada através de controles de acesso físico e do software de certificação, utilizando o tipo "n" pessoas de um grupo de "m".

6.2.2.2 É exigido a presença no mínimo de 2 (dois) detentores da chave de ativação ("n") de um grupo de 8 (oito) ("m") para a ativação da chave da AC DIGITAL MÚLTIPLA.

6.2.3 Custódia (*escrow*) de chave privada

A AC DIGITAL MÚLTIPLA não implementa a recuperação (*escrow*) de chaves privadas, isto é, não permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4 Cópia de segurança de chave privada

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

6.2.4.2 A AC DIGITAL MÚLTIPLA mantém cópia de segurança de sua própria chave privada.

6.2.4.3 A AC DIGITAL MÚLTIPLA não mantém cópia de segurança da chave privada de Titular de Certificado de assinatura digital por ela emitido.

6.2.4.4 Em qualquer caso, a cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1 As chaves privadas dos titulares de certificados emitidos pela AC DIGITAL MÚLTIPLA não são arquivadas.

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

6.2.6 Inserção de chave privada em módulo criptográfico

A AC DIGITAL 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 da chave privada da AC DIGITAL MÚLTIPLA é implementada por meio de módulo criptográfico, após identificação de 2 (dois) dos detentores da chave de ativação da chave criptográfica. As senhas utilizadas obedecem à política de senhas estabelecida pela AC DIGITAL MÚLTIPLA.

6.2.9 Método de desativação de chave privada

A chave privada da AC DIGITAL MÚLTIPLA que está armazenada em módulo criptográfico, é desativada quando não mais é necessária através de mecanismo disponibilizado pelo software de certificação que permite eliminar as informações contidas. Este procedimento é implementado por meio de módulos criptográficos, protegidos com senha, após a identificação de 2 (dois) dos detentores da chave de ativação da chave criptográfica. O espaço em disco onde eventualmente se encontrava a chave é subscrito.

6.2.10 Método de destruição de chave privada

Quando a chave privada da AC DIGITAL MÚLTIPLA for desativada, em decorrência de expiração ou revogação, esta é eliminada da memória do módulo criptográfico pelos Operadores da AC DIGITAL MÚLTIPLA, acompanhados de 2 (dois) dos detentores da chave criptográfica.

Todas as cópias de segurança são destruídas como todos os discos rígidos, tokens, módulos criptográficos e qualquer mídia de armazenamento que as tenha hospedado.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A AC DIGITAL MÚLTIPLA armazena as chaves públicas da própria AC DIGITAL MÚLTIPLA e dos titulares de certificado de assinatura digital, bem como as LCRs emitidas, 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 A chave privada da AC DIGITAL MÚLTIPLA e dos titulares de certificado por ela emitidos, são utilizadas apenas durante o período de validade dos certificados correspondentes. As chaves públicas emitidas pela AC DIGITAL MÚLTIPLA podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos certificados correspondentes.

6.3.2.2 Não se aplica.

6.3.2.3 Cada PC implementada pela AC DIGITAL 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 O período máximo de validade admitido para o certificado da AC DIGITAL 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 DIGITAL MAIS.

6.4 Dados de ativação

Nos itens a seguir são descritos os dados de ativação distintos das chaves criptográficas, que 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 da chave privada da AC DIGITAL MÚLTIPLA são únicos e aleatórios.

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

6.4.2 Proteção dos dados de ativação

6.4.2.1 Os dados de ativação da AC DIGITAL MÚLTIPLA são protegidos contra o uso não autorizado, por meios criptográficos individuais com senha 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 da entidade titular de certificado, são protegidos contra uso não autorizado.

6.4.3 Outros aspectos dos dados de ativação

Todos os aspectos acerca dos dados de ativação já foram tratados nos itens de 6.1 a 6.3.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1 A AC DIGITAL MÚLTIPLA garante que a geração de seu par de chaves é realizada em ambiente *off-line*, para impedir o acesso remoto não autorizado durante o processo.

6.5.1.2 Os requisitos de segurança computacional do equipamento computacional do equipamento onde são gerados os pares de chaves criptográficos dos titulares de certificados emitidos pela AC DIGITAL MÚLTIPLA estão descritos em cada PC implementada.

6.5.1.3 Os computadores servidores, utilizados pela AC DIGITAL MÚLTIPLA, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) controle de acesso aos serviços e perfis da AC DIGITAL MÚLTIPLA;
b) clara SEPARAÇÃO das tarefas e atribuições relacionadas a cada perfil qualificado da AC DIGITAL MÚLTIPLA;
c) uso de criptografia para segurança de base de dados, quando exigido pela classificação desuas informações;
d) geração e armazenamento de registros de auditoria da AC DIGITAL MÚLTIPLA;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
f) mecanismos para cópias de segurança (*backup*); e
g) acesso restrito aos bancos de dados da AC DIGITAL MÚLTIPLA.

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

6.5.1.5 Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações da DIGITAL MÚLTIPLA onde residem os equipamentos utilizados para operação da AC DIGITAL MÚLTIPLA, o equipamento que passou por manutenção é inspecionado e formatado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC DIGITAL MÚLTIPLA. Todos esses eventos são

registrados para fins de auditoria.

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

6.5.2 Classificação da segurança computacional

A segurança computacional da AC DIGITAL MÚLTIPLA segue as recomendações *Common Criteria*.

6.5.3 Controle de segurança para as Autoridades de Registro

6.5.3.1 Os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas ARs para os processos de validação e aprovação de certificados são os implementados pela própria AC DIGITAL MÚLTIPLA em concordância com o regulamento editado por instrução normativa da AC Raiz que define as características mínimas de segurança para as AR da ICP- Brasil.

6.5.3.2 Na Politica de Segurança adotada foi atendido o requisito mínimo estabelecido em regulamento editado por instrução normativa da AC Raiz que define as características mínimas de segurança para as AR da ICP-Brasil.

6.6 Controles Técnicos do Ciclo de Vida

Esta DPC descreve, quando aplicáveis, os controles implementados pela AC DIGITAL MÚLTIPLA e pelas ARs a ela vinculadas no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1 Controles de desenvolvimento de sistemas

6.6.1.1 A AC DIGITAL MÚLTIPLA adota o Sistema de Certificação Digital YWYRA e o HAWA, desenvolvido por entidades terceiras. 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 DIGITAL 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 DIGITAL MÚLTIPLA geram documentação suficiente para suportar avaliações externas de segurança dos componentes da AC DIGITAL MÚLTIPLA.

6.6.2 Controle de gerenciamento de segurança

6.6.2.1 As ferramentas e os procedimentos empregados pela AC DIGITAL MÚLTIPLA e ARs vinculadas para garantir que os seus sistemas e redes operacionais implementam os níveis configurados de segurança são, de avaliação de cada *release* da versão do sistema de AC e do sistema de AR empregado pela AC DIGITAL MÚLTIPLA, passando por um ambiente de homologação e somente após realização de teste o Gerente da AC dará o parecer para passar a produção.

6.6.2.2 A AC DIGITAL MÚLTIPLA, possui equipe própria de desenvolvimento que realiza formalmente o gerenciamento de configurações que deverá ser usada para a instalação e para a contínua manutenção de seus sistemas.

Toda a documentação gerada no processo de atualização, de passagem do estado *stagging*, que se trata de um

estado de amadurecimento da aplicação para que passe para a fase seguinte - homologação e produção, todo o processo é documentado e arquivado para consulta em auditoria, se for necessário. Todos os ambientes se encontram segregados entre si de forma a replicar um cenário real.

6.6.3 Controles de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na geração da LCR

Todas as LCRs geradas pela AC DIGITAL MÚLTIPLA, antes de publicadas, 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 Os controles relativos à segurança da rede da AC DIGITAL MÚLTIPLA, passam por possuir *firewalls*, dispositivos de rede multifuncionais, sistemas de controle de acesso, utilização de certificados como meio de autenticação e recursos similares.

6.7.1.2 Nos servidores e elementos de infraestrutura e proteção de rede, utilizados pela AC DIGITAL MÚLTIPLA, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

6.7.1.3 Todos servidores e elementos de infraestrutura e proteção de redes, tais como, roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS) localizados no segmento de rede que hospeda o sistema de certificação da AC DIGITAL MÚLTIPLA, 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 e 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 permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2 Firewall

6.7.2.1 Mecanismos de *firewall* estão implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Um *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 DIGITAL 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 tem capacidade de 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 ao firewall ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

6.7.3.2 O sistema de detecção de intrusão tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

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

6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, *firewalls* ou *IDS* – são registradas em arquivos para posterior análise, que poderá ser automatizada. O exame dos arquivos de registro é realizado diariamente e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 Carimbo do tempo

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC DIGITAL 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(s) de versão

Todos os certificados emitidos pela AC DIGITAL MÚLTIPLA implementam a versão 3 do padrão ITU X.509.

7.1.2 Extensões de certificados

A AC DIGITAL MÚLTIPLA não emite certificado de AC.

7.1.3 Identificadores de algoritmos

A AC DIGITAL MÚLTIPLA não emite certificado de AC.

7.1.4 Formatos de nome

A AC DIGITAL MÚLTIPLA não emite certificado de AC.

7.1.5 Restrições de nome

A AC DIGITAL MÚLTIPLA não emite certificado de AC.

7.1.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil após a conclusão do processo de credenciamento, é 2.16.76.1.1.166.

7.1.7 Uso da extensão "Policy Constraints"

A AC DIGITAL MÚLTIPLA não emite certificado de AC.

7.1.8 Sintaxe e semântica dos qualificadores de política

A AC DIGITAL MÚLTIPLA não emite certificado de AC.

7.1.9 Semântica de processamento para extensões criticas

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

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1 Nos itens seguintes estão descritos todas as extensões de LCR utilizadas pela AC DIGITAL MÚLTIPLA e a sua criticalidade.

7.2.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões de LCR, utilizadas pela AC DIGITAL MÚLTIPLA:

a) "***Authority Key Identifier***": contém o ***hash*** SHA-1 da chave pública da AC DIGITAL MÚLTIPLA; e
b) "***CRL Number***", **não crítica**: contém número sequencial para cada LCR emitida.

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

Não se aplica.

7.3.2 Extensão de OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 Frequência e circunstâncias das avaliações

A AC DIGITAL MÚLTIPLA entidade integrante da ICP-Brasil sofre 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, observando 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 da AC DIGITAL MÚLTIPLA são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP- BRASIL [3].

8.3 Relação do avaliador com a entidade avaliada

A auditoria da AC DIGITAL MÚLTIPLA integrante da ICP-Brasil é realizada pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizada, 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 da AC DIGITAL MÚLTIPLA estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil e com princípios e critérios definidos pelo WebTrust.

8.4.2

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

8.4.3

A AC DIGITAL MÚLTIPLA informa que as entidades da ICP-Brasil a ela diretamente vinculadas (AR e PSS), também receberam auditoria prévia, para fins de credenciamento, e que a AC DIGITAL 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

Em 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

Em 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

As tarifas referentes aos serviços de emissão e renovação de certificados serão definidas e aplicadas internamente pela AC DIGITAL MÚLTIPLA.

9.1.2 Tarifas de acesso ao certificado

Não **se aplica.**

9.1.3 Tarifas de revogação ou de acesso à informação de status

A AC DIGITAL MÚLTIPLA não implementa tarifas de revogação ou de acesso à informação de status de certificado.

9.1.4 Tarifas para outros serviços

As tarifas serão definidas internamente pela AC DIGITAL MÚLTIPLA.

9.1.5 Política de reembolso

Não se aplica.

9.2 Responsabilidade Financeira

A responsabilidade da AC DIGITAL MÚLTIPLA é verificada conforme previsto na legislação brasileira.

9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2 Outros ativos

Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.1.1 Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecidos à AC DIGITAL MÚLTIPLA e a AR vinculada são consideradas sigilosas, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

9.3.1.2 Como princípio geral, nenhum documento, informação ou registro fornecido à AC, ou AR vinculada deverá ser divulgado, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo

respectivo titular, na forma da legislação aplicável.

9.3.2 Informações fora do escopo de informações confidenciais

Os seguintes documentos da AC DIGITAL MÚLTIPLA e AR vinculada são considerados documentos não sigilosos:

a) os certificados e as LCR emitidos;
b) informações corporativas ou pessoais que façam parte de certificados, ou de diretórios públicos;
c) as PCs implementadas pela AC DIGITAL MÚLTIPLA;
d) a DPC da AC DIGITAL MÚLTIPLA;
e) versões públicas de Políticas de Segurança (PS);
f) a conclusão dos relatórios de auditoria.

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

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

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

9.3.2.3 A AC DIGITAL MÚLTIPLA poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados emitidos no âmbito da ICP-Brasil.

9.3.3 Responsabilidade em proteger a informação confidencial

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

9.3.3.2 A chave privada de assinatura digital da AC DIGITAL MÚLTIPLA, é gerada e mantida pela própria AC DIGITAL MÚLTIPLA, que é a responsável pelo seu sigilo. A divulgação ou utilização da chave privada de assinatura da AC DIGITAL MÚLTIPLA é da 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, 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 DIGITAL MÚLTIPLA assegura a proteção dos dados pessoais conforme sua Política de Privacidade.

9.4.2 Tratamento de informações como privadas

Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC

DIGITAL MÚLTIPLA é considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma de legislação aplicável.

9.4.3 Informações não consideradas privadas

Informações sobre revogação de usuários finais são fornecidos na LCR da AC DIGITAL MÚLTIPLA.

9.4.4 Responsabilidade para proteger a informação privada

A AC DIGITAL 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

Qualquer informação privada da AC DIGITAL MÚLTIPLA ou AR vinculada, somente será permitida a divulgação a terceiros mediante autorização formal do titular do certificado. As formas de autorização podem se apresentadas das seguintes formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado do titular, 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 DIGITAL MÚLTIPLA ou AR vinculada, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

As informações privadas ou confidenciais sob a aguarda da AC DIGITAL 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 de dados perante terceiros.

9.4.7 Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8 Informações a terceiros

Como diretriz geral nenhum documento, informação ou registro, sob a guarda da AC DIGITAL MÚLTIPLA ou AR vinculada, será fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizado para fazê-lo e esteja 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 DIGITAL MÚLTIPLA declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

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

9.6.1.2 Precisão da informação

A AC DIGITAL MÚLTIPLA implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC DIGITAL MÚLTIPLA, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequente e ARs vinculadas na forma de sua DPC, PCs e normas complementares.

9.6.1.3 Identificação do requerente

A AC DIGITAL MÚLTIPLA implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC DIGITAL MÚLTIPLA, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ARs vinculadas na forma de sua DPC, PCs e normas complementares.

9.6.1.4 Consentimento dos titulares

A AC DIGITAL MÚLTIPLA implementa termos de consentimentos ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5 Serviço

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

9.6.1.6 Revogação

A AC DIGITAL MÚLTIPLA revogará certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos documentos *Baseline Requirements.*

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

9.6.3.2 A AC DIGITAL MÚLTIPLA informará à AC Raiz qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

9.6.4 Declarações e garantias das terceiras partes

9.6.4.1 As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC; e
b) verificar, a qualquer tempo, a validade do certificado.

9.6.4.2 Um certificado emitido pela AC DIGITAL MÚLTIPLA é considerado válido quando:

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

9.6.4.3 A utilização ou aceitação de certificados sem a observância das providências descritas é deconta 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 DIGITAL 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 DIGITAL 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

A DPC da AC DIGITAL MÚLTIPLA 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

A DPC da AC DIGITAL MÚLTIPLA vigora por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.3 Efeitos de rescisão e sobrevivência

Os atos praticados na vigência da DPC da AC DIGITAL MÚLTIPLA 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 ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa 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 da AC DIGITAL MÚLTIPLA deverá ser submetida à AC Raiz.

9.12.2 Mecanismo de notificação e períodos

Mudança nesta DPC será publicada no site da AC DIGITAL MÚLTIPLA:

- http://repositorio.acdigital.com.br/docs/ac-digital-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 da AC DIGITAL MÚLTIPLA serão solucionados de acordo com a legislação vigente.

9.13.2

É estabelecido que a DPC da AC DIGITAL MÚLTIPLA não prevalecerá sobre as normas, critério, práticas e procedimentos da ICP-Brasil.

9.14 Lei aplicável

A DPC da AC DIGITAL MÚLTIPLA é regida pela legislação da República Federativa do Brasil, notadamentea Medida Provisória Nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

9.15 Conformidade com a Lei aplicável

A AC DIGITAL 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 da AC DIGITAL MÚLTIPLA representa as obrigações e deveres aplicáveis à AC DIGITAL MÚLTIPLA e AR. Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2 Cessão

Os direitos e obrigações previstos nesta DPC da AC DIGITAL MÚLTIPLA 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 da DPC da AC DIGITAL MÚLTIPLA 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

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/** publicaa versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001	DOC-ICP-02
[9]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DE TEMPO Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12
[1]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL Aprovado pela Resolução nº 10, de 14 de fevereiro de 2002	DOC-ICP-06

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

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

11 REFERÊNCIAS BIBLIOGRÁFICAS

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

ASSSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 111.515/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 PracticesFramework, november 2003.

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

RFC 5019, IETF – The lightweight Online Certificate Status Protocol (OCSP) Profile for High VolumesEnvoirments, september 2007.

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 Certificatemanagment Protocol (CMP), september 2012.

RFC 6960, IETF – Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP,june 2003.