DIGITALSIGN CERTIFICAÇÃO DIGITAL LTDA.
(AC DIGITALSIGN)

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

VERSÃO 8.0 – 11/03/2026

HISTÓRICO DE VERSÕES

Data	*Versão*	*Observações*
25/07/2012	0.0	Redação Inicial
25/06/2013	1.0	Revisão
22/09/2015	1.1	Revisão
18/10/2018	1.2	Revisão
25/02/2019	1.3	Revisão
10/04/2019	1.4	Revisão
07/04/2020	2.0	Adequações às Resoluções nº 151, 154 e 155
29/06/2020	3.0	Adequações às Resoluções nº 156, 164 e 167
30/10/2020	4.0	Adequações à Resolução nº 177
17/03/2021	5.0	Adequações à Resolução nº 181
11/01/2021	6.0	Adequações à Resolução nº 197
18/01/2023	7.0	Adequações à Resolução nº 204
11/03/2026	8.0	Adequações à Resolução nº 207 e 211

AVISO LEGAL

CONTEÚDO

1. INTRODUÇÃO

1.1. VISÃO GERAL

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

A AC DigitalSign está certificada em nível imediatamente subsequente ao da Autoridade Certificadora Principal da DigitalSign (AC DigitalSign ACP) certificada pela AC Raiz da ICP-Brasil.

1.1.2. A estrutura desta DPC está baseada no DOC-ICP-05 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Declarações de Prática de Certificação das Autoridades Certificadoras da ICP-Brasil. As referências a formulários presentes nesta DPC deverão ser entendidas também como referências a outras formas que a AC DigitalSign ou entidades a ela vinculadas possa vir a adotar.

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

1.1.4. AC DigitalSign mantém todas as informações da sua DPC sempre atualizadas.

1.1.5. Este documento está em conformidade com 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. Este documento é designado Declaração de Práticas de Certificação da Autoridade Certificadora DigitalSign e referida a seguir como "DPC da AC DigitalSign".

Este documento é identificado pela seguinte informação:

INFORMAÇÃO DO DOCUMENTO	
Versão/Edição	8.0
Data de Aprovação	11/03/2026
Data de Validade	Não aplicável
OID	2.16.76.1.1.51
Localização	http://www.digitalsigncertificadora.com.br/repositorio/ac

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

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. AUTORIDADES CERTIFICADORAS

O termo "Autoridade Certificadora" (AC) designa a entidade que emite e gere certificados digitais.

Esta DPC refere-se à Autoridade Certificadora "AC DigitalSign".

1.3.2. AUTORIDADES DE REGISTRO

1.3.2.1. A Autoridade de Registo (AR) é uma entidade que desempenha o papel de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação dos seus solicitantes em nome da AC.

As ARs vinculadas à AC DigitalSign estão relacionadas em (URL): http://repositorio.digitalsigncertificadora.com.br/ac

O URL referido contém:

a) relação de todas as AR credenciadas; e
b) relação das AR que se tenham descredenciado da cadeia da AC DigitalSign, com respetiva data do descredenciamento.

1.3.3. TITULARES DE CERTIFICADO

Titulares de Certificado Titulares de Certificados dessa AC são pessoas físicas e jurídicas, para a versão v1(PF e PJ A1, A3) e para a versão v2(PF exclusivamente A3 e PJ exclusivamente SE-S e SE-H), autorizados pela AR responsável a receber um certificado digital emitido pela AC, tanto para sua própria utilização ou para utilização em equipamentos ou aplicações.

1.3.4. PARTES CONFIÁVEIS

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

1.3.5. OUTROS PARTICIPANTES

1.3.5.1 A relação de todos os Prestadores de Serviço de Suporte - PSS, Prestadores de Serviços Biométricos - PSBios e Prestadores de Serviço de Confiança - PSC vinculados diretamente a AC DigitalSign e/ou por intermédio das suas AR é publicada em http://repositorio.digitalsigncertificadora.com.br/ac.

1.4. USABILIDADE DO CERTIFICADO

1.4.1. USO APROPRIADO DO CERTIFICADO

A AC DigitalSign implementa as seguintes Políticas de Certificado Digital:

Na cadeia de certificação V5 (AC DigitalSign e AC DigitalSign G2):

Política de Certificado	Nome	OID
Política de Certificado de Assinatura Digital Tipo A1 da AC DigitalSign	PC A1 da AC DigitalSign	2.16.76.1.2.1.41
Política de Certificado de Assinatura Digital Tipo A2 da AC DigitalSign	PC A2 da AC DigitalSign	2.16.76.1.2.2.8
Política de Certificado de Assinatura Digital Tipo A3 da AC DigitalSign	PC A3 da AC DigitalSign	2.16.76.1.2.3.39
Política de Certificado de Assinatura Digital Tipo A4 da AC DigitalSign	PC A4 da AC DigitalSign	2.16.76.1.2.4.17
Política de Certificado de Sigilo Tipo S1 da AC DigitalSign	PC S1 da AC DigitalSign	2.16.76.1.2.101.13
Política de Certificado de Sigilo Tipo S2 da AC DigitalSign	PC S2 da AC DigitalSign	2.16.76.1.2.102.7
Política de Certificado de Sigilo Tipo S3 da AC DigitalSign	PC S3 da AC DigitalSign	2.16.76.1.2.103.11
Política de Certificado de Sigilo Tipo S4 da AC DigitalSign	PC S4 da AC DigitalSign	2.16.76.1.2.104.8

Na cadeia de certificação V12 (AC DigitalSign G3):

Política de Certificado	Nome	OID
Política de Certificado de Assinatura Digital Tipo A3 da AC DigitalSign	PC A3 da AC DigitalSign	2.16.76.1.2.3.39
Política de Certificado de Assinatura Digital Tipo SE-S da AC DigitalSign	PC SE-S da AC DigitalSign	2.16.76.1.2.201.16
Política de Certificado de Assinatura Digital Tipo SE-H da AC DigitalSign	PC SE-H da AC DigitalSign	2.16.76.1.2.202.10

1.4.2. USO PROIBITIVO DO CERTIFICADO

Nas PC correspondentes estão relacionadas, quando cabíveis, as aplicações para as quais existem restrições ou proibições para o uso desses certificados.

1.5. POLÍTICA DE ADMINISTRAÇÃO

1.5.1. ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome: DigitalSign Certificação Digital LTDA

1.5.2. DADOS DE CONTATO

Endereço: Rua General Bertoldo Klinger, 111 – Paulicéia – São Bernardo do Campo/SP
Telefone: (55 11) 2666 7280
Página Web: www.digitalsigncertificadora.com.br
Email: suporte@digitalsigncertificadora.com.br

1.5.3. PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Fernando Moreira
Telefone: (55 11) 2666 7280
Email: suporte@digitalsigncertificadora.com.br

1.5.4. PROCEDIMENTOS DE APROVAÇÃO DA DPC

Esta DPC é aprovada pelo ITI.

Os procedimentos de aprovação da DPC da AC são estabelecidos a critério do CG da ICP-Brasil.

1.6. DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CMM-SEI	Capability Maturity Model do Software Engineering Institute

CMVP	Cryptographic Module Validation Program
CN	Common Name
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SSL	Secure Socket Layer
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. REPOSITÓRIOS

2.1.1 As obrigações do repositório da AC DigitalSign são:

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

2.1.2 O repositório da AC DigitalSign está disponível para consulta pública, através de protocolo http, em: http://repositorio.digitalsigncertificadora.com.br/ac.

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

Não há qualquer restrição ao acesso para consulta ao repositório.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não-autorizado.

Somente a AC DigitalSign, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas no seu repositório.

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

2.1.4 A AC DigitalSign disponibiliza os seguintes repositórios para distribuição de LCR:

- A AC DigitalSign (**G1**) disponibiliza 03 (três) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR:
  - http://www.digitalsigncertificadora.com.br/repositorio/ac/ACDIGITALSIGN.crl
  - http://www.digitaltrust.com.br/repositorio/ac/ACDIGITALSIGN.crl
  - http://repositorio.icpbrasil.gov.br/lcr/DigitalSign/ACDIGITALSIGN.crl
- A AC DigitalSign **G2** disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR:
  - http://www.digitalsigncertificadora.com.br/repositorio/ac/ACDIGITALSIGNG2.crl
  - http://www.digitaltrust.com.br/repositorio/ac/ACDIGITALSIGNG2.crl
- A AC DigitalSign (**G3**) disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR:
  - http://www.digitalsigncertificadora.com.br/repositorio/ac/ACDIGITALSIGNG3.crl
  - http://www.digitaltrust.com.br/repositorio/ac/ACDIGITALSIGNG3.crl

2.2. PUBLICAÇÃO DE INFORMAÇÃO DOS CERTIFICADOS

2.2.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC DigitalSign (http://repositorio.digitalsigncertificadora.com.br/ac), obedecendo as regras e os critérios estabelecidos nesta DPC.

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

2.2.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC DigitalSign (http://repositorio.digitalsigncertificadora.com.br/ac):

a) seu próprio certificado;
b) suas LCR;
c) esta DPC;
d) as PCs que implementa;
e) uma relação, regularmente atualizada, contendo as AR vinculadas e seus respectivos endereços; e
f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

A AC DigitalSign atualiza as informações descritas no item anterior logo que sejam geradas, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

Os certificados são publicados após emissão.

A LCR é publicada de acordo com o disposto no item 4.9.7, 4.9.8 e 4.10 desta DPC.

2.4. CONTROLES DE ACESSO

Não há qualquer restrição ao acesso para consulta às informações descritas no item 2.1 e 2.2 desta DPC.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não-autorizado. Há permissão somente de leitura.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. ATRIBUIÇÃO DE NOMES

3.1.1. TIPOS DE NOMES

3.1.1.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "*distinguished name*" do padrão ITU X.500.

3.1.1.2. Não se aplica.

3.1.2. NECESSIDADE DE NOMES SIGNIFICATIVOS

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

3.1.3. ANONIMATO OU PSEUDÔNIMO DOS TITULARES DO CERTIFICADO

Não se aplica.

3.1.4. REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES

3.1.4.1. Não se aplica.

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

3.1.5. UNICIDADE DE NOMES

Esta DPC estabelece que identificadores do tipo "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado emitido pela AC DigitalSign.

Para assegurar a unicidade do campo DN podem ser incluídos números ou letras adicionais ao nome de cada titular.

3.1.6. PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

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

3.1.7. RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS

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

3.2. VALIDAÇÃO INICIAL DE IDENTIDADE

Neste item e nos itens seguintes estão descritos em detalhe os requisitos e procedimentos utilizados pelas AR vinculadas à AC DigitalSign para a realização dos seguintes processos:

a) **Identificação e cadastro iniciais 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, 3.2.3 e 3.2.7, 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 A POSSE DE CHAVE PRIVADA

A AC verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. O descrito no RFC 4210, atualizada pela RFC 6712 é utilizado como referência para essa finalidade.

3.2.2. AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO

3.2.2.1. DISPOSIÇÕES GERAIS

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

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

3.2.2.1.3. Deverá feita a confirmação da identidade da organização e da pessoa física responsável pelo certificado, 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 uso do certificado.

NOTA 01: Poderá a AC DIGITALSIGN e as AR a ela vinculada solicitar uma assinatura manuscrita ao titular ou responsável pelo uso do certificado para comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

3.2.2.1.4. Fica dispensado o disposto no item 3.2.2.1.3, alíneas "b" e "c" caso o responsável pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos

documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

3.2.2.1.5. O disposto no item 3.2.2.1.3 poderá ser realizado:

a) mediante comparecimento presencial do responsável pelo certificado; ou

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

3.2.2.2. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

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

a) Relativos à sua habilitação jurídica:

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

   ii. se entidade privada:

      1. certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e

      2. documentos da eleição de seus representantes legais, quando aplicável;

b) Relativos a sua habilitação fiscal:

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

   ii. prova de inscrição no Cadastro Nacional de Obras – CNO.

NOTA 01: Essas confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

3.2.2.3. 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.

3.2.2.3.1 **Aplicado apenas para certificados emitidos na cadeia V5:** É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

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

3.2.2.3.2. **Aplicado apenas para certificados emitidos na cadeia V5:** 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 (Aplicado apenas para certificados emitidos na cadeia V5)**

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

Neste item são definidos os procedimentos empregados pelas AR vinculadas a uma AC para a identificação e cadastramento iniciais de um indivíduo na ICP-Brasil. Essa confirmação deverá ser realizada mediante a presença física do interessado ou por um dos procedimentos listados nas alíneas 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, interação, documentação e tratamento biométrico:

a) Não se aplica;

b) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz; ou

c) Não se aplica.

3.2.3.1. PROCEDIMENTO PARA IDENTIFICAÇÃO DE UM INDIVÍDUO

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

a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:

   i. Registro de Identidade, se brasileiro; ou

   ii. Título de Eleitor, com foto; ou

   iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou

   iv. Passaporte, se estrangeiro não domiciliado no Brasil

b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

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

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

3.2.3.1.2 Os documentos digitais deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos. Tal verificação fará parte do dossiê eletrônico do titular do certificado.

Na hipótese da identificação positiva, fica dispensada a etapa de verificação conforme o item 3.2.3.1.3.

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

a) por agente de registro distinto do que realizou a etapa de identificação;

b) pela AR ou AR própria da AC ou ainda AR própria do PSS da AC; e

c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

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

3.2.3.1.5 Não se aplica.

3.2.3.1.6 Não se aplica.

3.2.3.1.7 Não se aplica.

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

3.2.3.1.8.1 Não se aplica.

3.2.3.2. **Informações contidas no certificado emitido para um indivíduo (Aplicado apenas em certificados emitidos dentro da cadeia V5):**

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

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

3.2.3.2.2. **Aplicado apenas em certificados emitidos dentro da cadeia V5**: Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

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

3.2.3.2.3. **Aplicado apenas em certificados emitidos dentro da V5:** Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original.

Nota 1 - Aplicado apenas em certificados emitidos dentro da V5: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

Nota 2 – Aplicado apenas em certificados emitidos dentro da V5: O cartão CPF poderá ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.2.4. INFORMAÇÕES NÃO VERIFICADAS DO TITULAR DO CERTIFICADO

Não se aplica.

3.2.5. VALIDAÇÃO DAS AUTORIDADES

Não se aplica.

3.2.6. CRITÉRIOS PARA INTEROPERAÇÃO

Não se aplica.

3.2.7. AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO OU APLICAÇÃO

3.2.7.1. DISPOSIÇÕES GERAIS

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

3.2.7.1.2. Se o titular for pessoa física, deverá ser feita a confirmação da sua identidade na forma do item 3.2.3 e esta assinará o termo de titularidade de que trata o item 4.1.

3.2.7.1.3. Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e da pessoa física responsável pelo certificado, na forma do item 3.2.2.

3.2.7.1.4. Fica dispensada a observância do disposto no item 3.2.3.1 para certificados cujo titular seja pessoa física, caso a solicitação seja assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e cujos dados biométricos já tenham sido devidamente coletados.

3.2.7.1.5. Fica dispensada a observância do item 3.2.2.1.3, alíneas "b" e "c", para certificados cujo titular seja pessoa jurídica quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo A3 ou superior, cuja titularidade é da mesma pessoa física responsável legal da organização e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

3.2.7.2. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO OU APLICAÇÃO

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

3.2.7.2.2. Não se aplica.

3.2.7.3. AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTO PARA CERTIFICADO CF-E-SAT

Não se aplica.

3.2.7.4. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO SAT

Não se aplica.

3.2.7.5. AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTOS PARA CERTIFICADO OM-BR

Não se aplica.

3.2.7.6. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO METROLÓGICO

Não se aplica.

3.2.8. PROCEDIMENTOS COMPLEMENTARES

3.2.8.1 A AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro, bem como os Princípios e Critérios WebTrust.

3.2.8.2 Todo o processo de identificação do titular do certificado é 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. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.2.8.2.1 Não se aplica.

3.2.8.3 É mantido arquivo 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.

3.2.8.3.3 Não se aplica.

3.2.8.4 A AC DigitalSign 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 CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6] e em regulamento editado por instrução normativa da AC Raiz que defina 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.

3.2.8.4.2 Não se aplica.

3.2.9. PROCEDIMENTOS ESPECÍFICOS

3.2.9.1 Não se aplica.

3.2.9.2 Não se aplica.

3.2.9.3 Não se aplica.

3.2.9.4 Não se aplica.

3.2.9.5 Não se aplica.

3.2.9.6 Não se aplica.

3.2.9.7 Não se aplica.

3.2.9.8 Não se aplica.

3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1. Esta DPC estabelece os processos de identificação e confirmação do cadastro do solicitante, utilizados pela AC DIGITALSIGN para a geração de novo par de chaves e de seu correspondente novo certificado.

3.3.2. Este processo é conduzido segundo uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2, 3.2.3 ou 3.2.7;

b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, cujo certificado requisitado seja do mesmo nível de segurança ou inferior; ou

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

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

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante.

A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas.

O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3. Solicitações de revogação de certificados são registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. SOLICITAÇÃO DE CERTIFICADO

A solicitação de emissão de um Certificado Digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR vinculada. Todas as referências a formulário deverão ser entendidas também como referências a outras formas que a AR vinculada possa vir a adotar.

De entre os requisitos e procedimentos operacionais estabelecidos pela AC DigitalSign para as solicitações de emissão de certificado, estão:

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;

c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico;

d) o disposto na alínea 'b' e a assinatura do termo de titularidade, no caso de AR ELETRÔNICA, por se tratar de procedimento automatizado, sem intervenção de agente de registro, serão regulamentados por Instrução Normativa da AC Raiz;

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

4.1.1. QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO

A submissão da solicitação é feita 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. Os requisitos específicos associados a essas obrigações estão detalhados nas PC implementadas pela AC DigitalSign.

4.1.2.1. RESPONSABILIDADES DA AC

4.1.2.1.1 A AC DigitalSign responde pelos danos a que der causa.

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

4.1.2.1.3 Não se aplica.

4.1.2.2. OBRIGAÇÕES DA AC

As obrigações da AC DigitalSign são:

a) operar de acordo com esta DPC e com as PC que implementa;

b) gerar e gerenciar seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

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

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

f) distribuir seu próprio certificado;

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

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados emitidos;

j) emitir, gerenciar e publicar sua LCR e quando aplicável, disponibilizar consulta online de situação do certificado (*OCSP Online Certificate Status Protocol*);

k) publicar em sua página web esta DPC da AC DigitalSign e as PC que implementa;

l) publicar em sua página web as informações descritas no item 2.2.2 desta DPC;

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

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

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

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

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;

u) informar à terceira parte e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC;

v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;

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

x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada às ACs que utilizam de seus serviços; e

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

4.1.2.3. RESPONSABILIDADES DA AR

A AR será responsável pelos danos a que der causa.

4.1.2.4. OBRIGAÇÕES DAS AR

As obrigações das AR vinculadas à AC DigitalSign são:

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

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

c) encaminhar as solicitações de emissão ou de revogação de certificados à AC DigitalSign utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil;

d) informar os titulares de certificado a emissão ou a revogação de seus certificados;

e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido em regulamentos editados por instruções normativas da AC Raiz e as características mínimas de segurança para as AR da ICP-Brasil, bem como os Princípios e Critérios WebTrust para AR [5];

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

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

h) divulgar suas práticas, relativas à 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 e AR executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2. APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO

4.2.2.1 Não se aplica.

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

4.2.3. TEMPO PARA PROCESSAR A SOLICITAÇÃO DE CERTIFICADO

A AC DigitalSign cumpre os procedimentos determinados na ICP-Brasil. Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3. EMISSÃO DE CERTIFICADO

4.3.1. AÇÕES DA AC DURANTE A EMISSÃO DE UM CERTIFICADO

4.3.1.1. A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento do "Termo de Titularidade" no caso de certificados de pessoas jurídicas, equipamentos ou aplicações e dos demais documentos exigidos.

Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido.

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

4.3.2. NOTIFICAÇÕES PARA O TITULAR DO CERTIFICADO PELA AC NA EMISSÃO DO CERTIFICADO

A emissão dos certificados para pessoas físicas ou jurídicas é feita na presença física, ou pelo próprio titular/responsável do certificado.

4.4. ACEITAÇÃO DE CERTIFICADO

4.4.1. CONDUTA SOBRE A ACEITAÇÃO DO CERTIFICADO

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

4.4.1.2. A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado, pessoa física responsável no caso de o certificado ser emitido a pessoa jurídica, na primeira utilização da chave privada correspondente.

4.4.1.3. Não se aplica.

4.4.2. PUBLICAÇÃO DO CERTIFICADO PELA AC

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

4.4.3. NOTIFICAÇÃO DE EMISSÃO DO CERTIFICADO PELA AC RAIZ PARA OUTRAS ENTIDADES

Não se aplica.

4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

A AC DigitalSign e o titular do certificado para usuário final devem operar de acordo com a esta Declaração de Práticas de Certificação (DPC), estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1. USABILIDADE DA CHAVE PRIVADA E DO CERTIFICADO DO TITULAR

4.5.1.1 A AC DigitalSign utiliza sua chave privada e garante a proteção dessa chave conforme o previsto nesta DPC.

4.5.1.2. OBRIGAÇÕES DO TITULAR DO CERTIFICADO

As obrigações dos titulares de certificados emitidos pela AC DigitalSign, constantes dos termos de titularidade de que trata o item 4.1, são:

a) fornecer, de modo completo e preciso, todas as informações necessárias para a 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 por esta DPC, pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;

e) informar à AC DigitalSign o comprometimento ou suspeita de comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente; e

f) garantir a proteção do PUK, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente.

Nota: Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, 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 item 3.3 desta DPC.

4.6.1. CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPC.

4.6.2. QUEM PODE SOLICITAR A RENOVAÇÃO

Em acordo com item 3.3 desta DPC.

4.6.3. PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS

Em acordo com item 3.3 desta DPC.

4.6.4. NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR

Em acordo com item 3.3 desta DPC.

4.6.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO

Em acordo com item 3.3 desta DPC.

4.6.6. PUBLICAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO PELA AC

Não se aplica.

4.6.7. NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES

Em acordo com item 4.3 desta DPC.

4.7. NOVA CHAVE DE CERTIFICADO (RE-KEY)

4.7.1. CIRCUNSTÂNCIAS PARA NOVA CHAVE DE CERTIFICADO

Não se aplica.

4.7.2. QUEM PODE REQUISITAR A CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA

Não se aplica.

4.7.3. PROCESSAMENTO DE REQUISIÇÃO DE NOVAS CHAVES DE CERTIFICADO

Não se aplica.

4.7.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR

Não se aplica.

4.7.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA NOVA CHAVE CERTIFICADA

Não se aplica.

4.7.6. PUBLICAÇÃO DE UMA NOVA CHAVE CERTIFICADA PELA AC

Não se aplica.

4.7.7. NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES

Não se aplica.

4.8. MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.1. CIRCUNSTÂNCIAS PARA MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.2. QUEM PODE REQUISITAR A MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.3. PROCESSAMENTO DE REQUISIÇÃO DE MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR

Não se aplica.

4.8.5. CONDUTA CONSTITUINDO A ACEITAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO

Não se aplica.

4.8.6. PUBLICAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO PELA AC

Não se aplica.

4.8.7. NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES

Não se aplica.

4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO

4.9.1.1. O TITULAR DO CERTIFICADO E O RESPONSÁVEL PELO CERTIFICADO PODEM SOLICITAR A REVOGAÇÃO DO SEU CERTIFICADO EM QUALQUER ALTURA E INDEPENDENTEMENTE DE QUALQUER CIRCUNSTÂNCIA.

4.9.1.2. O certificado é obrigatoriamente revogado:

a) quando for constatada emissão imprópria ou defeituosa do mesmo;

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

c) no caso de extinção, dissolução ou transformação da AC DigitalSign; ou

d) no caso de comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora.

4.9.1.3. A AC DigitalSign revoga, no prazo definido no item 4.4.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil.

O CG da ICP-Brasil ou AC Raiz determina a revogação do certificado da AC DigitalSign quando essa deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.9.1.4. Todo certificado deverá ter a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado.

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

4.9.2. QUEM PODE SOLICITAR REVOGAÇÃO

A revogação de um certificado somente poderá ser feita:

a) por solicitação do titular do certificado;

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

c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;

d) Pela AC DigitalSign;

e) Por uma AR vinculada;

f) Por determinação do CG da ICP-Brasil ou da AC Raiz;

g) Não se aplica;

h) Não se aplica;

i) Não se aplica;

j) Não se aplica.

4.9.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.9.3.1. É necessária uma solicitação de revogação para que AR responsável inicie o processo de revogação.

As instruções para a solicitação de revogação do Certificado são obtidas em página web disponibilizada pela AC DigitalSign ou pela AR Responsável.

A revogação é realizada através de formulário contendo o motivo da solicitação de revogação e mediante o fornecimento de dados indicados na solicitação de emissão do certificado, ou por formulário assinado pelo titular na falta desses dados.

4.9.3.2. Como diretrizes gerais:

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

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

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

d) O processo final de revogação de um certificado termina com a geração e a publicação da LCR que contenha o certificado revogado e com a atualização do estado do certificado em resposta OCSP à base de dados da AC DigitalSign, quando aplicável.

4.9.3.3. O prazo máximo para conclusão do processo de revogação do certificado pela AC DigitalSign, após a conclusão do processo de aceitação e registro da solicitação de revogação é de 24 (vinte e quatro) horas.

4.9.3.4. Não se aplica.

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

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.

O prazo para aceitação do certificado pelo seu titular é de 3 (três) dias, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

4.9.4.2. Não se aplica.

4.9.5. TEMPO EM QUE A AC DEVE PROCESSAR O PEDIDO DE REVOGAÇÃO

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

4.9.6. REQUISITOS DE VERIFICAÇÃO DE REVOGAÇÃO PARA AS PARTES CONFIÁVEIS

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

4.9.7. FREQUÊNCIA DE EMISSÃO DE LCR

4.9.7.1. A frequência para emissão de LCR referentes a certificados de usuários finais é de 1 (uma) hora, podendo ser estendida em casos excepcionais até ao limite estabelecido no item 4.9.7.2.

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

4.9.7.3. Não se aplica.

4.9.7.4. Não se aplica.

4.9.8. LATÊNCIA MÁXIMA PARA A LCR

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

4.9.9. DISPONIBILIDADE PARA REVOGAÇÃO OU VERIFICAÇÃO DE STATUS ON-LINE

A AC DigitalSign suporta os processos de revogação de certificados de forma online quando aplicável por força de contratação específica.

A verificação da situação de um certificado deverá ser feita diretamente na AC DigitalSign, por meio do protocolo OCSP (On-line Certificate Status Protocol).

4.9.10. REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE

Não se aplica.

4.9.11. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

Não se aplica.

4.9.12. REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE

4.9.12.1. O titular de certificado deve notificar imediatamente, através de solicitação de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada.

4.9.12.2. A perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de chave deve ser comunicado à AC DigitalSign através do formulário específico para tal fim.

4.9.13. CIRCUNSTÂNCIAS PARA SUSPENSÃO

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

4.9.14. QUEM PODE SOLICITAR SUSPENSÃO

A AC DigitalSign, 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 DigitalSign fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados ou OCSP, 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 Em caso de extinção da AC DigitalSign, AR Vinculada ou PSS serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.11.2. Os procedimentos incluem, mas não estão limitados à divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, aplicativos dedicados à certificação digital, guarda de bases de dados e registros observará os mesmos requisitos de segurança exigidos pela AC DigitalSign.

4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVE

4.12.1. POLÍTICA E PRÁTICAS DE CUSTÓDIA E RECUPERAÇÃO DE CHAVE

Não é permitida a recuperação (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

4.12.2. POLÍTICA E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVE DE SESSÃO

Não se aplica.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1. CONTROLES FÍSICOS

5.1.1. CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES

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

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

a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;

b) Instalações para sistemas de telecomunicações;

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

d) Iluminação de emergência.

5.1.2. ACESSO FÍSICO NAS INSTALAÇÕES DE AC

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

5.1.2.1. NÍVEIS DE ACESSO

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

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

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

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

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

não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

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

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

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC DigitalSign tais como emissão e revogação de certificados e emissão de LCR e a disponibilidade à resposta a consulta OCSP. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver sendo ocupado.

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

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

5.1.2.1.11. Na AC DigitalSign, existe 1 (um) ambiente de quarto nível para abrigar e segregar:

a) equipamentos de produção on-line;

b) equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores;

c) equipamentos de produção off-line e cofre de armazenamento.

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

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

a) confeccionado em aço;

b) possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) consiste em pequenos depósitos localizados no interior do cofre de Nível 5. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da chave privada da AC DigitalSign são armazenados nesses depósitos.

5.1.2.2. SISTEMAS FÍSICOS DE DETECÇÃO

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmaras de vídeo ligadas a um sistema de gravação 24x7.

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da

fita) trimestralmente, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

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

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

5.1.2.2.6. O sistema de monitoramento das câmaras de vídeo, bem como o sistema de notificação de alarmes estão localizados em ambiente de nível 3 e são permanentemente monitorados. As instalações do sistema de monitoramento estão sendo monitoradas, por sua vez, por câmara de vídeo que permite acompanhar as ações.

5.1.2.3. SISTEMA DE CONTROLE DE ACESSO

O sistema de controle de acesso está baseado no ambiente de nível 4.

5.1.2.4. MECANISMOS DE EMERGÊNCIA

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

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

5.1.3. ENERGIA E AR CONDICIONADO

5.1.3.1. A infraestrutura do ambiente de certificação da AC DigitalSign está dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC DigitalSign e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC DigitalSign.

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

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

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

5.1.3.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela Política de Segurança da ICP-Brasil. Qualquer modificação nessa rede é previamente documentada.

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

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

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

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

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

a) gerador de porte compatível;

b) gerador 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 e infiltrações provenientes de qualquer fonte externa.

5.1.5. PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO

5.1.5.1. Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

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

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

5.1.6. ARMAZENAMENTO DE MÍDIA

A AC DigitalSign atende às normas NBR 11.515 e 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 magnéticos 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

As instalações de backup (*Disaster Recovery*) atendem os requisitos mínimos estabelecidos por este documento. A 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

5.2.1. PERFIS QUALIFICADOS

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

5.2.1.2. A AC DigitalSign estabelece diferentes perfis 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 detalhe dos perfis encontra-se em documento interno normativo.

5.2.1.3. Todos os operadores do sistema de certificação da AC DigitalSign recebem formação específica antes de obter qualquer tipo de acesso. O tipo e o nível de acesso estão determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4. A AC DigitalSign possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos seus funcionários. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o funcionário devolve à AC DigitalSign no ato de seu desligamento.

5.2.2. NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

5.2.2.1. É requerido um controle multiusuário para a geração e a utilização da chave privada da AC DigitalSign, 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 DigitalSign requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC podem ser executadas por um único empregado.

5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

5.2.3.1. Todo empregado da AC DigitalSign tem a sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso às instalações da AC DigitalSign;

b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC DigitalSign;

c) receber um certificado para executar suas atividades operacionais na AC DigitalSign;

d) receber uma conta no sistema de certificação da AC DigitalSign.

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

a) são diretamente atribuídos a um único empregado;

b) não são compartilhados;

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

5.2.3.3. A AC DigitalSign implementa um padrão de utilização de "senhas fortes", definido na Política de Segurança implementada e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas.

5.2.4. FUNÇÕES QUE REQUEREM SEPARAÇÃO DE DEVERES

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

5.3. CONTROLES DE PESSOAL

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

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.

5.3.1. ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE

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

5.3.2. PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

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

a) verificação de antecedentes criminais;

b) verificação de situação de crédito;

c) verificação de histórico de empregos anteriores; e

d) comprovação de escolaridade e de residência.

5.3.2.2. Não se aplica.

5.3.3. REQUISITOS DE TREINAMENTO

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

a) princípios e mecanismos de segurança da AC DigitalSign e das AR vinculadas;

b) sistema de certificação em uso na AC DigitalSign;

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 3.2.7;

e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA

O pessoal da AC DigitalSign e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre mudanças tecnológicas nos sistemas da AC DigitalSign.

5.3.5. FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

Não estabelecido.

5.3.6. SANÇÕES PARA AÇÕES NÃO AUTORIZADAS

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

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

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

b) identificação dos envolvidos;

c) eventuais prejuízos causados;

d) punições aplicadas, se for o caso;

e) conclusões.

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

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

a) advertência;

b) suspensão por prazo determinado;

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

5.3.7. REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

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

5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.3.8.1. A AC DigitalSign disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas:

a) a DPC da AC DigitalSign;

b) não se aplica;

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

d) documentação operacional relativa às suas atividades;

e) contratos, normas e políticas relevantes para as suas atividades.

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

5.4. PROCEDIMENTOS DE LOG DE AUDITORIA

5.4.1. TIPOS DE EVENTOS REGISTRADOS

5.4.1.1. A AC DigitalSign registra em arquivos de auditoria todos os eventos relacionados com a segurança do seu sistema de certificação. Os seguintes eventos são 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 DigitalSign;

c) mudanças na configuração dos sistemas AC DigitalSign ou nas suas chaves;

d) mudanças nas políticas de criação de certificados;

e) tentativas de acesso (login) e de saída do sistema (logoff);

f) tentativas não-autorizadas de acesso aos arquivos do sistema;

g) geração de chaves próprias da AC DigitalSign;

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.

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

a) registros de acessos físicos;

b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e perfis qualificados;

d) relatórios de discrepância e comprometimento;

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

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

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

5.4.1.5. A documentação relacionada aos serviços da AC DigitalSign é armazenada em local único, de forma estruturada para facilitar o acesso e consulta nos processos de auditoria, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.4.1.6. As AR vinculadas à AC DigitalSign registram eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são incluídos em arquivos de auditoria:

a) os agentes de registro que realizaram as operações;

b) data e hora das operações;

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

d) a assinatura digital do executante.

5.4.1.6.1 Não se aplica.

5.4.1.7. A AC DigitalSign define, em documento disponível nas auditorias de conformidade, o local de arquivo dos dossiês dos titulares.

5.4.2. FREQUÊNCIA DE AUDITORIA DE REGISTROS

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

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

5.4.3. PERÍODO DE RETENÇÃO PARA REGISTROS DE AUDITORIA

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

5.4.4. PROTEÇÃO DE REGISTRO DE AUDITORIA

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

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

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

5.4.5. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTRO DE AUDITORIA

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC DigitalSign têm cópias de segurança semanais, efetuadas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas.

5.4.6. SISTEMA DE COLETA DE DADOS DE AUDITORIA (INTERNO OU EXTERNO)

O sistema de recolha de dados de auditoria interno à AC DigitalSign é uma combinação de processos automatizados e manuais, executada pelo seu pessoal operacional e/ou pelos seus sistemas.

5.4.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

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

5.4.8. AVALIAÇÕES DE VULNERABILIDADE

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

5.5. ARQUIVAMENTO DE REGISTROS

5.5.1. TIPOS DE REGISTROS ARQUIVADOS

a) solicitações de certificados;

b) solicitações e justificativas 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 DigitalSign;

g) informações de auditoria previstas no item 5.4.1.

5.5.2. PERÍODO DE RETENÇÃO PARA ARQUIVO

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

b) os dossiês dos titulares são retidos por 7 (sete) anos, a contar da data de expiração ou revogação do certificado;

c) as demais informações, inclusive os arquivos de auditoria, são retidas por 7 (sete) anos.

5.5.3. PROTEÇÃO DE ARQUIVO

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

5.5.4. PROCEDIMENTOS PARA CÓPIA DE ARQUIVO

5.5.4.1. A AC DigitalSign estabelece que uma segunda cópia de todo o material arquivado é armazenada no site *Disaster Recovery*, 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 DigitalSign verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. REQUISITOS PARA DATAÇÃO DE REGISTROS

As informações de data e hora nos registros baseiam-se no horário Greenwich Mean Time.

Nos casos em que, por algum motivo, os documentos formalizem o uso de outro formato, ele será aceito.

5.5.6. SISTEMA DE COLETA DE DADOS DE ARQUIVO (INTERNO OU EXTERNO)

Todos os sistemas de coleta de dados de arquivo utilizados pela AC DigitalSign nos seus procedimentos operacionais são automatizados e manuais e internos.

5.5.7. PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO

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

5.6. TROCA DE CHAVE

5.6.1. O titular do certificado pode solicitar um novo certificado antes da data de expiração do seu certificado ainda válido, através de formulário específico, disponibilizado pela AR Responsável, por onde é encaminhado o processo de fornecimento de novo certificado.

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

A comunicação de expiração, juntamente com as instruções para a solicitação de um novo certificado é realizada através de correio eletrônico enviado ao titular do certificado.

5.6.2. Não se aplica.

5.7. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

A AC DigitalSign possui um Plano de Continuidade de Negócios testado anualmente para garantir a continuidade de seus serviços críticos.

5.7.1. PROCEDIMENTOS GERENCIAMENTO DE INCIDENTE E COMPROMETIMENTO

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

A AC DigitalSign testa, revisa e atualiza anualmente esses procedimentos. O Plano de Continuidade de Negócios inclui, de entre outras:

a) As condições para ativar o plano;

b) Procedimentos de emergência;

c) Procedimentos de fallback;

d) Procedimentos de restauração;

e) Cronograma para manutenção do plano;

f) Requisitos de conscientização e educação;

g) Responsabilidades individuais;

h) Objetivo de Tempo de Recuperação (RTO);

i) Testes regulares dos planos de contingência;

j) O plano para manter ou restaurar as operações de negócios da AC DigitalSign de forma oportuna, após a interrupção ou falha de processos críticos de negócios;

k) Definição de requisitos para armazenar materiais criptográficos críticos em um local alternativo;

l) Definição de interrupções aceitáveis do sistema e um tempo de recuperação;

m) Frequência para realização de cópias de backup;

n) Distância entre as instalações de recuperação e o site principal da AC Raiz; e

o) Procedimentos para proteger suas instalações após um desastre e antes de restaurar o ambiente seguro no local original ou remoto.

5.7.1.2. As AR vinculadas à AC DigitalSign possuem um Plano de Continuidade de Negócios testado anualmente para garantir a recuperação, total ou parcial das atividades das AR, contendo, no mínimo as seguintes informações:

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

b) identificação e concordância de todas as responsabilidades e procedimentos de emergência;

c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial é dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;

d) documentação dos processos e procedimentos acordados;

e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;

f) teste e atualização dos planos.

5.7.2. RECURSOS COMPUTACIONAIS, SOFTWARE, E DADOS CORROMPIDOS

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Administrador de Segurança da AC DigitalSign, que decreta o início da fase de resposta.

Nessa fase, é realizada uma rigorosa inspeção para verificar a veracidade do fato e as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação.

Caso haja necessidade, o administrador de Segurança decretará a contingência respectiva.

5.7.3. PROCEDIMENTOS NO CASO DE COMPROMETIMENTO DE CHAVE PRIVADA DE ENTIDADE

5.7.3.1. CERTIFICADO DE ENTIDADE É REVOGADO

Em caso de revogação do certificado da AC DigitalSign o Administrador de Segurança, juntamente com o Administrador PKI da AC DigitalSign, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados.

A AC DigitalSign gerará novo par de chaves da AC DigitalSign, e logo que tenha sido emitido o certificado associado ao novo par de chaves gerado, a AC DigitalSign emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

5.7.3.2. CHAVE DA ENTIDADE É COMPROMETIDA

Em caso de suspeita de comprometimento de chave da AC DigitalSign, o fato é imediatamente comunicado ao Administrador de Segurança que, juntamente com o Administrador PKI da AC DigitalSign, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e a AC DigitalSign, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados.

A AC DigitalSign gerará novo par de chaves da AC DigitalSign, e logo que tenha sido emitido o certificado associado ao novo par de chaves gerado, a AC DigitalSign emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

5.7.4. CAPACIDADE DE CONTINUIDADE DE NEGÓCIO APÓS DESASTRE

Em caso de desastre natural ou de outra natureza, é notificado o Administrador de Segurança, que decreta o início da fase de resposta.

Nessa fase, é realizada uma rigorosa inspeção para verificar as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação.

Caso haja necessidade, as atividades são transferidas para o site de *Disaster Recovery*.

5.8. EXTINÇÃO DA AC

Em caso de extinção da AC DigitalSign, AR Vinculada ou PSS serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

Os procedimentos incluem, mas não estão limitados à divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, aplicativos dedicados à certificação digital, guarda de bases de dados e registros observará os mesmos requisitos de segurança exigidos pela AC DigitalSign.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1. GERAÇÃO DO PAR DE CHAVES

6.1.1.1. O par de chaves criptográficas da AC DigitalSign é gerado pela própria AC DigitalSign, após ter sido deferido o seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. A geração do par de chaves de AC DigitalSign é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança, treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria. O par de chaves da AC DigitalSign é gerado em módulo criptográfico que adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

Os pares de chaves criptográficas são gerados somente pelo titular do certificado correspondente.

Os procedimentos específicos estão descritos em cada PC implementada pela AC DigitalSign.

6.1.1.3. Cada PC implementada pela AC DigitalSign define 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. As chaves da AC DigitalSign são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.1.1.6. O módulo criptográfico de geração de chaves assimétricas da AC DigitalSign adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.2. ENTREGA DA CHAVE PRIVADA À ENTIDADE

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

6.1.3. ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

6.1.3.1. A AC DigitalSign entrega cópia de sua chave pública à AC DigitalSign ACP em formato PKCS #10.

6.1.3.2. Os procedimentos para a entrega da chave pública de um solicitante de certificado estão detalhados nas PC implementadas.

6.1.4. ENTREGA DE CHAVE PÚBLICA DA AC ÀS TERCEIRAS PARTES

A AC DigitalSign disponibiliza o seu certificado e todos os certificados da cadeia de certificação para os usuários da ICP-Brasil, de entre outras, através do seu diretório.

6.1.5. TAMANHOS DE CHAVE

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

6.1.5.2. Não se aplica.

6.1.6. GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

6.1.6.1. Os parâmetros de geração de chaves assimétricas da AC DigitalSign adotam o padrão RSA 4096, conforme padrão 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 em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

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

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

6.2. PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

A AC DigitalSign implementa uma combinação de controles físicos, lógicos e procedimentais de forma a garantir a segurança das suas chaves privadas. As chaves privadas da AC DigitalSign trafegam cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento. Cada PC implementada especifica os requisitos específicos aplicáveis para a proteção das chaves privadas das entidades titulares de certificados.

6.2.1. PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC DigitalSign adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.1.2. Cada PC implementada especifica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.2.2. CONTROLE "N DE M" PARA CHAVE PRIVADA

6.2.2.1. A AC DigitalSign exige controle múltiplo do tipo "n de m" para utilização da sua chave privada.

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

6.2.3. CUSTÓDIA (*ESCROW*) DE CHAVE PRIVADA

Não é permitida a recuperação (*escrow*) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

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

6.2.4.2. A AC DigitalSign mantém cópia de segurança de sua chave privada.

6.2.4.3. A AC DigitalSign não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.5. ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1. Não devem ser arquivadas chaves privadas de assinatura digital.

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

6.2.6. INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

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

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

6.2.7. ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Ver item 6.1.

6.2.8. MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

A ativação das chaves privadas das AC DigitalSign é coordenada pelo seu Administrador PKI, implementando-se o controle "n de m", conforme item 6.2.2 anterior. A identidade dos intervenientes é verificada por guarda armado.

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

6.2.9. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

A desativação das chaves privadas das AC DigitalSign é coordenada pelo seu Administrador PKI, implementando-se o controle "n de m", conforme item 6.2.2 anterior. A identidade dos intervenientes é verificada por guarda armado.

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

6.2.10. MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

A destruição das chaves privadas das AC DigitalSign é coordenada pelo seu Administrador PKI, implementando-se o controle "n de m", conforme item 6.2.2 anterior. A identidade dos intervenientes é verificada por guarda armado.

As mídias de armazenamento das chaves privadas são reinicializadas de forma a não restarem nelas informações sensíveis.

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

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. ARQUIVAMENTO DE CHAVE PÚBLICA

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

6.3.2. PERÍODOS DE OPERAÇÃO DO CERTIFICADO E PERÍODOS DE USO PARA AS CHAVES PÚBLICA E PRIVADA

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

6.3.2.2. Cada PC implementada pela AC DigitalSign 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].

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

6.4. DADOS DE ATIVAÇÃO

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Cada PC implementada descreve os requisitos específicos aplicáveis.

6.4.1. GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

6.4.1.1. Os dados de ativação dos equipamentos criptográficos que armazenam as chaves privadas da AC DigitalSign são únicos e aleatórios.

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

6.4.2. PROTEÇÃO DOS DADOS DE ATIVAÇÃO

6.4.2.1. A AC DigitalSign garante que os dados de ativação de sua chave privada são protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

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

6.4.3. OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO

Não se aplica.

6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1. REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

6.5.1.1. A geração do par de chaves da AC DigitalSign é realizada em ambiente de nível 4. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não autorizado.

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

6.5.1.3. O ambiente computacional da AC DigitalSign relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes funções:

a) controle de acesso aos serviços e perfis da AC DigitalSign;

b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC DigitalSign;

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

d) geração e armazenamento de registros de auditoria da AC DigitalSign;

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

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

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

6.5.1.5. As informações sensíveis contidas nos equipamentos são retiradas dos equipamentos para manutenção. Os números de série dos equipamentos e as datas de envio e de recebimento da manutenção são controlados. Ao retornar às instalações da AC DigitalSign, o equipamento que passou por manutenção é inspecionado.

As informações sensíveis armazenadas, relativas à atividade da AC DigitalSign, são destruídas de maneira definitiva nos equipamentos que deixam de ser utilizados em caráter permanente.

Todos esses eventos são registados para fins de auditoria.

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

6.5.2. CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL

A segurança computacional da AC DigitalSign segue as recomendações Common Criteria.

6.5.3. CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO

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

6.5.3.2. Os requisitos correspondem, no mínimo, aos especificados em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

6.5.3.3. Não se aplica.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.6.1.1. A AC DigitalSign utiliza preferencialmente sistemas e tecnologias certificadas. Quaisquer desenvolvimentos e/ou customizações são realizadas em ambiente de desenvolvimento/homologação antes da sua passagem a produção.

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

6.6.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA

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

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

b) a administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional e pelos papéis confiados descritos nesta DPC.

6.6.2.2. A AC DigitalSign utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação da AC DigitalSign, incluindo:

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

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

c) instalação de novos serviços na plataforma de processamento.

6.6.3. CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA

Não se aplica.

6.6.4. CONTROLES NA GERAÇÃO DE LCR

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

6.7. CONTROLES DE SEGURANÇA DE REDE

6.7.1. DIRETRIZES GERAIS

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

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

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

6.7.1.4. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes

são implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

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

6.7.2. FIREWALL

6.7.2.1. Os mecanismos de *firewall* são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. O *firewall* promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (*DMZ*) – em relação aos equipamentos com acesso exclusivamente interno à AC DigitalSign.

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

6.7.3. SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS)

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

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

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

6.7.4. REGISTRO DE ACESSOS NÃO-AUTORIZADOS À REDE

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

6.8. CARIMBO DE TEMPO

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. PERFIL DO CERTIFICADO

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

7.1.1. NÚMERO DE VERSÃO

Todos os certificados emitidos pela AC DigitalSign implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2. EXTENSÕES DE CERTIFICADO

A ICP-Brasil define como obrigatórias as extensões para certificados de AC conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I do DOCICP-04, aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.

7.1.3. IDENTIFICADORES DE ALGORITMO

Não se aplica.

7.1.4. FORMATOS DE NOME

O nome da AC titular de certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I do DOC-ICP-04, aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.

7.1.5. RESTRIÇÕES DE NOME

Não se aplica.

7.1.6. OID (OBJECT IDENTIFIER) DA DPC

O OID desta DPC é 2.16.76.1.1.51.

7.1.7. USO DA EXTENSÃO "POLICY CONSTRAINTS"

Não se aplica.

7.1.8. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Não se aplica.

7.1.9. SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2. PERFIL DE LCR

7.2.1. NÚMERO(S) DE VERSÃO

As LCR geradas pela AC DigitalSign 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. A DPC implementa todas as extensões de LCR utilizadas e a sua criticidade, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I do DOC-ICP-04, aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.

Para certificados emitidos na cadeia V5: Neste item são descritas todas as extensões de LCR utilizadas pela AC DigitalSign e sua criticalidade.

7.2.2.2. **Aplicado apenas em certificados emitidos dentro da cadeia V5:** A ICP-Brasil define como obrigatórias, e são implementadas pela AC DigitalSign, as seguintes extensões de LCR:

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

7.3. PERFIL DE OCSP

7.3.1. NÚMERO(S) DE VERSÃO

Serviços de respostas OCSP deverão implementar a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. EXTENSÕES DE OCSP

Em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

As entidades integrantes da ICP-Brasil sofrem auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento.

8.2. IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

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

8.2.2. Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas 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

As auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO

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

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

8.4.3 As entidades da ICP-Brasil diretamente vinculadas a AC DigitalSign – AR e PSS, também receberam auditoria prévia, para fins de credenciamento, e a AC DigitalSign 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

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

9.1.2. TARIFAS DE ACESSO AO CERTIFICADO

Não são cobradas tarifas de acesso ao certificado digital emitido.

9.1.3. TARIFAS DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS

Pela revogação ou acesso à informação de status do certificado será cobrado o valor estabelecido contratualmente.

9.1.4. TARIFAS PARA OUTROS SERVIÇOS

Pelos demais serviços será cobrado o valor estabelecido contratualmente.

9.1.5. POLÍTICA DE REEMBOLSO

Em caso de revogação do certificado por motivo de comprometimento da chave privada ou da mídia armazenadora da chave privada da AC DigitalSign, ou ainda quando constatada a emissão imprópria ou defeituosa imputável à AC DigitalSign, será emitido gratuitamente outro certificado em substituição.

9.2. RESPONSABILIDADE FINANCEIRA

A responsabilidade da AC DigitalSign 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, todos os documentos, informações ou registros fornecidos à AC ou às AR são sigilosos.

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

9.3.2. INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS

Não são consideradas informações sigilosas:

a) os certificados e LCR/OCSP emitidos pela AC DigitalSign;

b) informações corporativas ou pessoais que constem nos certificados ou em diretórios públicos;

c) as PC implementadas pela AC;

d) esta DPC;

e) versões públicas de Políticas de Segurança;

f) resultados finais de auditorias.

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

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

a) qualquer PC aplicável;

b) qualquer DPC;

c) versões públicas de Política de Segurança – PS; e

d) a conclusão dos relatórios da auditoria.

9.3.2.3. A AC DigitalSign também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo 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 devem possuir mecanismos para assegurar a proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

9.3.3.2. AC DigitalSign gera e mantém sua chave privada, sendo responsável pelo seu sigilo. A divulgação ou utilização indevida da sua chave privada é da sua inteira responsabilidade.

9.3.3.3. Os titulares (ou os responsáveis no caso de pessoa jurídica) dos certificados de assinatura emitidos pela AC DigitalSign são responsáveis pela geração, manutenção e sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevida dessas mesmas chaves.

9.4. PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1. PLANO DE PRIVACIDADE

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

9.4.2. TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS

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

9.4.3. INFORMAÇÕES NÃO CONSIDERADAS PRIVADAS

Informações sobre revogação de certificados de usuários finais são fornecidas na LCR/OCSP da AC DigitalSign.

9.4.4. RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADAS

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

9.4.5. AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS

As informações privadas obtidas pela AC DigitalSign poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável.

O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou

b) por meio de pedido escrito com firma reconhecida.

9.4.6. DIVULGAÇÃO EM PROCESSO JUDICIAL OU ADMINISTRATIVO

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

As informações privadas ou confidenciais sob a guarda da AC DigitalSign poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7. OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO

Não se aplica.

9.4.8. INFORMAÇÕES A TERCEIROS

Nenhum documento, informação ou registro sob a guarda da AC DigitalSign é fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, através de instrumento devidamente constituído, estiver corretamente identificada e autorizada para o fazer.

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 declara e garante o quanto segue:

9.6.1.1. AUTORIZAÇÃO PARA CERTIFICADO

A AC DigitalSign implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC DigitalSign, no âmbito da

autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das ARs vinculadas na forma de suas DPCs, PCs e normas complementares.

9.6.1.2. PRECISÃO DA INFORMAÇÃO

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

9.6.1.3. IDENTIFICAÇÃO DO REQUERENTE

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

9.6.1.4. CONSENTIMENTO DOS TITULARES

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

9.6.1.5. SERVIÇO

A AC DigitalSign mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios e LCRs/OCSP.

9.6.1.6. REVOGAÇÃO

A AC DigitalSign irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos Princípios e Critérios WebTrust.

9.6.1.7. EXISTÊNCIA LEGAL

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

9.6.2. DECLARAÇÕES E GARANTIAS DA AR

Em acordo com item 4 desta DPC.

9.6.3. DECLARAÇÕES E GARANTIAS DO TITULAR

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

9.6.3.2. A AC DigitalSign deve informar 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;

b) verificar, a qualquer tempo, a validade do certificado.

9.6.4.2. Um certificado emitido pela AC DigitalSign é considerado válido quando:

i. tiver sido emitido pela AC DigitalSign;

ii. não constar como revogado pela AC DigitalSign;

iii. não estiver expirado; e

iv. puder ser verificado com uso do certificado válido da AC emitente.

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

9.6.5. REPRESENTAÇÕES E GARANTIAS DE OUTROS PARTICIPANTES

Não se aplica.

9.7. ISENÇÃO DE GARANTIAS

Não se aplica.

9.8. LIMITAÇÕES DE RESPONSABILIDADES

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

9.10. PRAZO E RESCISÃO

9.10.1. PRAZO

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

9.10.2. TÉRMINO

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

9.10.3. EFEITO DA RESCISÃO E SOBREVIVÊNCIA

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

9.11. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por escrito e entregue à AC DigitalSign.

9.12. ALTERAÇÕES

9.12.1. PROCEDIMENTOS PARA EMENDAS

Qualquer alteração nesta DPC é submetida à aprovação do CG da ICP-Brasil.

9.12.2. MECANISMO DE NOTIFICAÇÃO E PERÍODOS

Mudança nesta DPC será publicado no site da AC DigitalSign.

9.12.3. CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO

Não se aplica.

9.13. SOLUÇÃO DE CONFLITOS

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

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

9.14. LEI APLICÁVEL

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

9.15. CONFORMIDADE COM A LEI APLICÁVEL

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

9.16. DISPOSIÇÕES DIVERSAS

9.16.1. ACORDO COMPLETO

Esta DPC representa as obrigações e deveres aplicáveis à AC DigitalSign e AR vinculadas. 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 são de ordem pública e indisponíveis, não podendo ser cedidos ou transferidos a terceiros.

9.16.3. INDEPENDÊNCIA DE DISPOSIÇÕES

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

9.16.4. EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)

De acordo com a legislação vigente.

9.17. OUTRAS PROVISÕES

Não se aplica.

10. DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[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 DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12
[1]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL Aprovado pela Resolução nº 10, de 14 de fevereiro de 2002	DOC-ICP-06

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

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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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

RFC 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, 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 Certificate Management Protocol (CMP), september 2012.

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