Declaração de Práticas de Certificação

da

Autoridade Certificadora

SAFE-ID BRASIL

Assinatura Geral e
Proteção de e-mail (S/MIME)

(DPC AC SAFE-ID BRASIL)

Versão 2.1 de Agosto de 2025

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Responsável	Motivo	Descrição
1.0	Agosto/2021	Lucia Castelli	Versão Inicial	Versão inicial compatível com a versão 6.1 do DOC-ICP-05(DPC) - https://www.iti.gov.br
1.0	Agosto/2021	Alice Vasconcellos	Aprovação	
2.0	Setembro/2022	Fernando Morgado	Alterações	Adequação as resoluções 197 e 204
2.0	Setembro/2022	Alice Vasconcellos	Aprovação	
2.1	Agosto/2025	Fernando Morgado	Alterações	Item 3.1.1.1 - Alteração do texto (alinea a) e alinea b).
2.1	Agosto/2025	Alice Vasconcellos	Aprovação	

1. INTRODUÇÃO

1.1.Visão Geral

1.1.1. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da Empresa SAFE-ID BRASIL CERTIFICACAO DIGITAL EIRELI credenciada como AC SAFE-ID BRASIL, Autoridade Certificadora (AC) integrante da infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na execução dos seus serviços.

1.1.2. A DPC da AC SAFE-ID BRASIL adota obrigatoriamente a mesma estrutura empregada no documento DOC-ICP-05.

1.1.3. Não se aplica.

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

1.1.5. A AC SAFE-ID BRASIL mantém todas as informações da sua DPC sempre atualizadas.

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

1.2. Nome do documento e Identificação

1.2.1. Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora SAFE-ID BRASIL”, integrante da ICP-Brasil, e comumente referida como “DPC AC SAFE-ID BRASIL”. O Identificador de Objeto (OID) desta DPC é **2.16.76.1.1.155**.

1.2.2. A AC SAFE-ID BRASIL emite certificados para usuários finais, exclusivamente para assinatura de documento e proteção de e-mail (S/MIME).

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

Esta DPC se refere unicamente à AC SAFE-ID BRASIL, integrante da ICP-Brasil.

1.3.2. Autoridades de Registro

1.3.2.1. O endereço da página *web* (URL) da AC é https://certificados.serpro.gov.br/acsafeidbrasil.

Neste endereço está publicado dados referentes à Autoridade de Registro responsável pelo processo de recebimento, identificação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

a) relação de todas as AR credenciadas;

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

1.3.3. Titulares de Certificado

Titulares de Certificados são as entidades – pessoas físicas ou jurídicas - 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

A AC SAFE-ID BRASIL utiliza o Serviço Federal de Processamento de dados (SERPRO) como Prestador de Serviço de Suporte – PSS, Prestador de Serviço Biométrico – PSBio e Prestador de Serviço de Confiança - PSC conforme disponibilizado no endereço: https://certificados.serpro.gov.br/acsafeidbrasil.

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

As Políticas de Certificado (PC) implementadas pela AC, são:

PC AC SAFE-ID BRASIL A1	**OID 2.16.76.1.2.1.121**
PC AC SAFE-ID BRASIL A3	**OID 2.16.76.1.2.3.114**

As PCs definem como os certificados emitidos são utilizados pela comunidade.

Nas PCs estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC.

1.4.2. Uso proibitivo do certificado

As aplicações para as quais são adequados os certificados emitidos pela AC e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso destes certificados, estão relacionadas na Política de Certificado correspondente.

1.5. Política de Administração

Esta DPC é administrada pela própria AC SAFE-ID BRASIL.

1.5.1. Organização Administrativa do documento

Autoridade Certificadora SAFE-ID BRASIL.

1.5.2. Contatos

Administrativo:

Nome: ÂNGELA SOUZA MAIA

Endereço: SHN Quadra 01, Bloco A – Sala 1218 – Asa Norte – Brasília//DF

CEP: 70.701-000

E-mail: angela.maia@safeidbrasil.com.br

Telefone: (61) 98227-8925

Suporte / Fraudes

Nome: Central de Serviços SERPRO

Página Web: https://atendimento.serpro.gov.br/certificacaodigital

E-mail: css.serpro@serpro.gov.br

Telefone: 0800 7282323

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

Nome: ÂNGELA SOUZA MAIA

Telefone: (61) 98227-8925

E-mail: angela.maia@safeidbrasil.com.br

1.5.4. Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

1.6. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AGR	Agente de Registro
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF PKIX	*Internet Engineering Task Force - Public-Key Infrastructured (X.509)*

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	*Online Certificate Status Protocol*
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade do Negócio
PIN	Personal Identification Number
PIS	Programa de Integração Social
POP	*Proof of Possession*
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
PUK	PIN Unblocking Key
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SNMP	*Simple Network Management Protocol*
UF	Unidade de Federação
URL	Uniform Resource Location

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1. Obrigações:

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

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

c) Implementar os recursos necessários e garante a segurança dos dados nele armazenados.

2.1.2. Os requisitos aplicáveis aos repositórios da AC estão abaixo descritos:

a) Localização Física: Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

Para os certificados emitidos pela AC, tem-se os repositórios nos seguintes endereços:

http://repositorio.serpro.gov.br/lcr/acsafeidbrasil.crl http://certificados2.serpro.gov.br/lcr/acsafeidbrasil.crl

b) Disponibilidade conforme referida no item 2.2.1;

c) Protocolos de acesso – HTTP e HTTPS;

d) Requisitos de segurança:

i. Os servidores físicos estão situados em ambiente de segurança nível 4 conforme definido no item – obedece aos requisitos definidos no item 5.1.2.1.7;

ii. A frequência de backup é diária;

iii. Os procedimentos de manutenção e os perfis técnicos de operação estão formalmente definidos;

iv. Os registros de logs são auditados conforme a frequência definida no item 5.4.2 desta DPC;

v. São realizadas análises periódicas de vulnerabilidades;

vi. A arquitetura segurança para proteção de perímetro está composta por: Firewall, IPS e AntiDDoS;

vii. A monitoração dos eventos de segurança ou indisponibilidade é realizada por equipe especializada em regime 24x7.

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

2.1.4. A AC SAFE-ID BRASIL disponibiliza 02(dois) repositórios em infraestruturas de rede segregadas, para distribuição de LCR, conforme abaixo:

http://repositorio.serpro.gov.br/lcr/acsafeidbrasil.crl http://certificados2.serpro.gov.br/lcr/acsafeidbrasil.crl

2.2. Publicação de informações dos certificados

2.2.1. A AC publica e mantém disponível em sua página *web* as informações descritas no endereço https://certificados.serpro.gov.br/acsafeidbrasil.

A disponibilidade da página é de no mínimo 99,5% (noventa e nove vírgula cinco por cento) no mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2. As seguintes informações são publicadas na página *web*;

a) seu próprio certificado;

b) suas LCRs;

c) sua DPC;

d) as PCs que implementam essa AC;

e) relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços; e

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

2.3. Tempo ou Frequência de Publicação

Os certificados e a LCR são publicados imediatamente após sua emissão pela AC. As demais informações mencionadas no item 2.2.2 serão publicadas sempre que sofrerem alterações.

2.4. Controle de Acesso aos Repositórios

Não existe nenhuma restrição ao acesso para consulta a esta DPC, às suas PCs, aos certificados emitidos e a LCR da AC. Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis, designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Atribuição de Nomes

3.1.1. Tipos de nomes

3.1.1.1. Os tipos de nomes admitidos para os titulares de certificados da AC são:

a) Certificados de pessoa física, o campo ”Common name” (CN) é é composto do nome da pessoa física e o número de inscrição da pessoa física do titular do certificado.

b) Certificados de pessoa jurídica, o campo ”Common name” (CN) é composto do nome empresarial da pessoa jurídica e o número de inscrição da empresa titular do certificado.

3.1.1.2. Não se aplica.

3.1.2. Necessidade dos nomes serem significativos

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

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. Os requisitos e procedimentos específicos, quando aplicáveis, estão detalhados nas PCs implementadas.

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

3.1.5. Unicidade de nomes

Os identificadores do tipo "*Distinguished name*" (DN) são únicos para cada titular de certificados no âmbito da AC SAFE-ID BRASIL. Números ou letras adicionais são incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6. Procedimento para resolver disputa de nomes

A AC reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes. Durante o processo de confirmação de identidade, cabe ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

A DPC estabelece que 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 seguintes a DPC descreve os requisitos e os procedimentos gerais para a primeira identificação, e cadastramento junto à ICP-Brasil de pessoas titulares ou responsáveis por certificados digitais para a realização dos seguintes processos:

a) Identificação do titular do certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.2.2 e 3.2.3.

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

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: após a conferência dos dados da solicitação de certificado com os constantes dos documentos e biometrias apresentados, na etapa de identificação, é liberada a 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 são verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

3.2.1. Método para comprovar o controle da chave privada

A confirmação de que a entidade solicitante controla a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 4210, relativos a POP (*Proof of Possession*).

3.2.2. Autenticação da identificação da organização

3.2.2.1. Disposições Gerais

3.2.2.1.1. Os procedimentos empregados pela AR vinculada para a confirmação da identidade de uma pessoa jurídica é feita mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

3.2.2.1.2. É 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. É 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 digital de titularidade de que trata o item 4.1. pelo titular ou responsável pelo uso do certificado.

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

3.2.2.1.4. Não se aplica;

3.2.2.1.5 O disposto no item 3.2.2.1.3 é 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 é feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos a sua habilitação jurídica:

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

ii. Se entidade privada:

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

2. Documentos da eleição de seus 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 Específico do INSS – CEI.

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

3.2.2.3. Informações contidas no certificado emitido para uma organização

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

a) Nome empresarial constante do CNPJ (cadastro nacional de Pessoa Jurídica), sem abreviações[1];

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

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

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

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

3.2.2.4. Responsabilidade decorrente do uso do certificado de uma organização

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

3.2.3. Autenticação da identidade de um indivíduo

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

a) por módulo de AR eletrônico, exclusivamente nos casos previstos neste regulamento;

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

1 No campo Subject, como parte do Common Name, que compõe o Distinguished Name
2 No campo Subject Alternative Name, OID 2.16.76.1.3.3
3 No campo Subject Alternative Name, OID 2.16.76.1.3.2
4 No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.4

3.2.3.1. Procedimento para identificação de um indivíduo

A identificação da pessoa física requerente do certificado é 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 defini 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 é 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 são 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. Os documentos em papel, os quais não existem formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, são 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 observa 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 é realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICPBrasil, que deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade.

3.2.3.1.8.1. Não se aplica.

3.2.3.2. Informações contidas no certificado emitido para um indivíduo

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

a) nome completo, sem abreviações[1];

b) data de nascimento[2].

c) Cadastro de Pessoa Física[3]

3.2.3.2.1.1. Não se aplica.

3.2.3.2.2. Cada PC define como obrigatório o preenchimento de outros campos ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, solicita 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 Para tanto, o titular apresenta a documentação respectiva, caso a caso em sua versão original.

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

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

3.2.3.2.3.1. Não se aplica

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 um equipamento ou aplicação

3.2.7.1. Disposições Gerais

1 No campo Subject, como parte do Common Name, que compõe o Distinguished Name.
2 No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.1.
3 CPF

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

3.2.7.5. Procedimentos para efeitos de identificação de um equipamento SAT

Não se aplica.

3.2.7.6. Informações contidas no certificado emitido para um equipamento SAT

Não se aplica.

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

Não se aplica.

3.2.7.8. Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

3.2.7.9. Informações contidas no certificado emitido para um equipamento metrológico

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 da Webtrust para Autoridades Certificadoras disponíveis em http://www.webtrust.org, bem como da norma ISO/IEC 270001:2013.

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. O sistema biométrico da ICP-Brasil solicita aleatoriamente qual dedo o AGR deve apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGR no cadastro do sistema biométrico. Tais registros 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 são mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-Brasil[1].

3.2.8.3.1. Não se aplica.

3.2.8.3.2. Não se aplica

3.2.8.3.3. Não se aplica

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

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

3.2.8.4.2. Não se aplica

3.2.9. Procedimentos específicos

3.2.9.1. Não se aplica.

3.2.9.2. Não se aplica.

3.2.9.3. Não se aplica.

3.2.9.4. 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. Neste item a DPC estabelece os processos de identificação e confirmação do cadastro do solicitante, utilizados pela AC SAFE-ID BRASIL para a geração de novo par de chaves e de seu correspondente novo certificado.

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

a) Adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e, 3.2.3.

b) A solicitação por meio eletrônico, na página da AR, opção “Meu certificado/Renovar”, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja pelo menos do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;

c) Não se aplica;

d) Não se aplica;

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

f) Não se aplica.

3.3.2.1 Não se aplica.

3.3.3. Não existem procedimentos específicos nas PCs implementadas.

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 na página da AR emissora do certificado, permitindo a identificação inequívoca do solicitante.

A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas. O procedimento para solicitação de revogação de certificado emitido pela AC está descrito no item 4.9.3 desta DPC.

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

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

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. Solicitação de Certificado

Os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado são:

a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.2;

b) Mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; e

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

d) Não se aplica.

Nota 1: Não se aplica.

Nota 2: Não se aplica.

4.1.1. Quem pode submeter uma solicitação de certificado

A submissão da solicitação é 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 são descritas as obrigações gerais das entidades envolvidas.

4.1.2.1. Responsabilidades da AC

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

4.1.2.1.2. A AC 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

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. As obrigações específicas para as PCs implementadas, estão descritas nas PCs, no item correspondente.

a) Operar de acordo com DPC da AC e com as PCs que implementa;

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

c) Assegurar a proteção de suas chaves privadas;

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

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

f) Distribuir o seu próprio certificado;

g) Emitir, expedir e distribuir os certificados de AR a ela vinculadas e de usuários finais;

h) Informar a emissão do certificado ao respectivo solicitante;

i) Revogar os certificados por ela emitidos;

j) Emitir, gerenciar e publicar suas LCR e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - *On-line Certificate Status Protocol*);

k) Publicar na página *web* a DPC e as PCs aprovadas que implementa;

l) Publicar, na página *web*, as informações definidas no item 2.2.2. deste documento;

m) Publicar, na página *web*, informações sobre o descredenciamento de AR;

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

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

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

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

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

s) manter e testar anualmente seu Plano de continuidade do Negócio - PCN;

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

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

v) Informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos 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 é responsável pelos danos a que der causa.

4.1.2.4. Obrigações da AR

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

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

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

c) Encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-Brasil[1];

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

e) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC SAFE-ID BRASIL e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARS DA ICP-BRASIL [1], bem como os Princípios e Critérios WebTrust para AR [5];

f) Manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;

g) Proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2. e 3.2.3. e

h) Divulgar suas práticas, relativas a cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR [5].

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

A AC 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 aceitam ou rejeitam, com a devida justificativa formal, 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 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. Os certificados são emitidos pela AC de acordo com os seguintes passos:

a) O responsável pela AR verifica o completo e correto preenchimento da solicitação do certificado, bem como a documentação do solicitante;

b) O responsável pela AR aprova a solicitação, disponibilizando o certificado para a instalação por seu solicitante;

c) O software de AC emite automaticamente um *e-mail* informando ao solicitante que o certificado está disponível para instalação.

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

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

O software de AC emite automaticamente um e-mail informando ao solicitante que o certificado está disponível para instalação conforme item 4.3.1.1.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.1.1. O recebimento de um certificado pelo Titular de Certificado e o uso subsequente das chaves e certificado, constitui aceitação do certificado por parte do Titular de Certificado. Aceitando um certificado, o Titular de Certificado:

a) Concorda estar de acordo com as responsabilidades contínuas, obrigações e deveres impostas a ele pelo Termo de responsabilidade e PC implementada pela AC e esta DPC;

b) Garante que por seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado;

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

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

4.4.1.3. Não se aplica.

4.4.2. Publicação do certificado pela AC

O certificado da AC são publicados de acordo com item 2.2 desta DPC.

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

Não se aplica.

4.5. Usabilidade do par de chaves e do certificado

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

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.1.1. A AC 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 do titular de certificado emitido de acordo com esta DPC e constantes dos termos de titularidade de que trata o item 4.1, são as abaixo relacionadas:

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

b) Garantir a proteção e o sigilo de suas chaves privadas, código de ativação (PIN) e dispositivos criptográficos;

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

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

e) Informar à AC SAFE-ID BRASIL qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

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 assinatura de código, 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. A AC revoga um certificado por ela emitido pelos seguintes motivos:

a) Solicitação de revogação corretamente preenchida pelo Titular do Certificado;

b) Solicitação de revogação enviada à AC por um terceiro autorizado, por exemplo, uma determinação judicial;

c) Solicitação de revogação feita por uma pessoa com procuração do Titular do Certificado;

d) Titular de Certificado deixa a comunidade de interesses sob a qual seu certificado foi emitido, por exemplo:

- Titular de Certificado organizacional deixa o emprego;
- Ocorre o falecimento do Titular de Certificado;

4.9.1.2. Um certificado é revogado obrigatoriamente pelos seguintes motivos.

a) Quando constatada emissão imprópria ou defeituosa do mesmo;

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

c) No caso de dissolução de AC; ou

d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3. Em relação à revogação, ainda é observado que:

a) A AC SAFE-ID BRASIL revoga, no prazo definido no item 4.9.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil; e

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

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

4.9.1.4.1. Não se aplica.

4.9.1.4.2. Não se aplica.

4.9.1.5. A autenticidade da LCR é também confirmada por meio das verificações da assinatura da AC SAFE-ID BRASIL e do período de validade da LCR.

4.9.2. Quem pode solicitar revogação

A solicitação para a revogação de um certificado somente é 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 SAFE-ID BRASIL;

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. A AC garante que todos agentes habilitados, conforme o item 4.9.2, podem, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados.

4.9.3.2. Como diretrizes gerais, fica estabelecido que:

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

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

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

d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado.

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

4.9.3.4. Não se aplica.

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

4.9.3.6. Não existem procedimentos de revogação específicos para as PCs implementadas.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação é imediata quando configuradas as circunstâncias definidas no item 4.9.1. A AC estabelece o prazo de 7(sete) dias para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado é solicitada sem cobrança de tarifa pela AC.

4.9.4.2. Não são requeridos prazos específicos para as PCs implementadas por esta AC.

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 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 confirma 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 identificadas em cada certificado na cadeia de certificação.

A autenticidade da LCR também é confirmada por meio da verificação da assinatura da AC e do período de validade da LCR.

4.9.7. Frequência de emissão de LCR

4.9.7.1. A frequência de emissão de LCR referentes a certificados de usuários finais é de 1 (uma) hora.

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

4.9.7.3. Não se aplica.

4.9.7.4. Não se aplica.

4.9.7.5. Não se aplica.

4.9.8. Latência máxima para a LCR

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

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

Não se aplica.

4.9.10. Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11. Outras formas disponíveis para divulgação de revogação

4.9.11.1. A AC não suporta outras formas para divulgação da revogação que não através da publicação de LCR.

4.9.11.2. Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. Quando houver comprometimento ou suspeita de comprometimento da chave privada, o Titular do Certificado comunica imediatamente a AC SAFE-ID BRASIL.

4.9.12.2. A comunicação a AC é através de formulário específico disponibilizado na página (Solicitação de Revogação) da AC.

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

Não se aplica.

4.9.15. Procedimento para solicitação de suspensão

Não se aplica.

4.9.16. Limites no período de suspensão

Não se aplica.

4.10. Serviços de status de certificado

4.10.1. Características operacionais

A AC fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR.

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. Caso seja necessária a extinção dos serviços de AC ou AR, a AC efetuará os procedimentos aplicáveis descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-Brasil [6].

4.11.2. Os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivos, incluem:

a) Notificação para o e-mail do titular do certificado.

b) Transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta;

c) Preservação de quaisquer registros não transferidos a um sucessor.

d) As chaves públicas dos certificados emitidos pela AC dissolvida serão armazenadas por outra AC após aprovação da AC Raiz.

e) Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC.

f) A AC, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

g) Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

Não se aplica.

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

Não se aplica.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

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

5.1. Controles Físicos

5.1.1. Construção e localização das instalações de AC

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

5.1.1.2. Todos os aspectos de construção das instalações da AC, relevantes para os controles de segurança física, foram executados por técnicos especializados, e passam por manutenção periodica, especialmente as instalações abaixo:

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 e estabilizadores e similares;

b) Instalações para sistemas de telecomunicações;

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

d) Iluminação de emergência.

O ambiente principal de produção é situado em sala-cofre construída de acordo com os requisitos da norma ABNT e acreditada pelo INMETRO. Assim, possui todos os dispositivos exigidos em norma, tais como: controladora de temperatura/umidade, placa controladora, condensadora, evaporadora, painel de detecção e alarme endereçável com fontes de alimentação e conjunto de baterias, detector de fumaça dentre outros.

5.1.2. Acesso físico

O acesso físico às dependências da AC é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-Brasil [8].

5.1.2.1. Níveis de Acesso

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

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC. 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 transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC 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, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem 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 nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico, e o uso de crachá.

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

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

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

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

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

5.1.2.1.11. São três os tipos de serviço abrigados no ambiente de quarto nível:

a) Equipamentos de produção online e cofre de armazenamento;

b) Equipamentos de produção offline e cofre de armazenamento;

c) Equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

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

5.1.2.1.13. Para garantir a segurança do material armazenado, os cofres obedecem às seguintes especificações mínimas:

a)Ser feito em aço ou material de resistência equivalente; e

b)Possuir tranca com chave.

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

5.1.2.2.2. As mídias de armazenamento 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 mídia pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) mídia referente a cada semana. Essas mídias são armazenadas em ambiente de terceiro nível.

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

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

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

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

5.1.2.3. Sistema de Controle de Acesso

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

5.1.2.4. Mecanismos de emergência

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

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

5.1.3. Energia e ar-condicionado

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

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

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

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

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

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

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

5.1.3.8. A temperatura dos ambientes de nível 4, site principal e de backup, 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 é garantida por meio de:

a) Geradores de porte compatível;

b) Geradores de reserva;

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

d) Sistemas redundantes de ar-condicionado.

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio

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

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

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

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

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

5.1.6. Armazenamento de mídia

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

5.1.7. Destruição de lixo

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

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

5.1.8. Instalações de segurança (*backup*) externas (*offsite*) para AC

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

5.2. Controles Procedimentais

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

5.2.1. Perfis qualificados

5.2.1.1. A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregada estão limitadas de acordo com o seu perfil.

5.2.1.2. A AC estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. Os perfis específicos, bem como as respectivas responsabilidades estão descritas no Manual de Segurança do Centro de Certificação Digital do SERPRO. A saber:

a) Gerente do SGSI;

b) Gerente do CCD-SERPRO;

c) Gestor de Software;

d) Administrador de Segurança;

e) Administrador do Sistema de Gerenciamento de Certificados;

f) Administrador do Sistema Operacional;

g) Segurança patrimonial

h) Apoio administrativo;

i) Administrador de Conformidade; e

j) Administrador de Software.

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

5.2.1.3.1 Não aplicável.

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

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC 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 necessitam da presença de no mínimo 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC são executadas por um único operador.

5.2.3. Identificação e autenticação para cada perfil

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

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

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

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

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

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

a) São diretamente atribuídos a um único operador (funcionário da AC devidamente qualificado);

b) Não são compartilhados; e

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

5.2.3.3. A AC implementa um padrão de utilização de “senhas fortes”, definido na sua Política de Segurança (PS) em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], junto a procedimentos de validação dessas senhas.

5.2.4. Funções que requerem separação de deveres

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

5.3. Controles de Pessoal

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

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

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

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

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC e AR vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. São definidos requisitos adicionais para a admissão.

5.3.2. Procedimentos de Verificação de Antecedentes

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

a) Verificação de antecedentes criminais;

b) Verificação de situação de crédito;

c) Verificação de histórico de empregos anteriores; e

d) Comprovação de escolaridade e de residência;

5.3.2.2. A AC defini requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

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

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

b) Sistema de certificação em uso na AC;

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

d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.2.2 e 3.2.3; e

e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

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

5.3.5. Frequência e sequência de rodízios de cargos

A AC não implementa rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. A AC, na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC ou de uma AR vinculada, suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação, instaurar processo administrativo para apurar os fatos e, se for o caso, adotará as medidas legais cabíveis.

5.3.6.2. O processo administrativo referido acima 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

e) Conclusões.

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

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

a) Advertência;

b) Suspensão por prazo determinado; ou

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

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC e das ARs vinculadas, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é

contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC poderá definir requisitos adicionais para a contratação.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC disponibiliza para todo o seu pessoal e para o pessoal das ARs vinculadas, pelo menos:

a) Esta DPC;

b) As PCs que implementa;

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

d) Documentação operacional relativa às suas atividades;

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

5.3.8.2. Toda a documentação é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC.

5.4. Procedimentos de *Log* de auditoria

Nos itens seguintes esta DPC descreve os aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC com o objetivo de manter um ambiente seguro.

5.4.1. Tipos de Evento Registrados

5.4.1.1. Todas as ações executadas pelo pessoal da AC, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A AC registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

a) Iniciação e desligamento do sistema de certificação;

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

c) Mudanças na configuração da AC ou nas suas chaves;

d) Mudanças nas políticas de criação de certificados;

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

f) Tentativas não-autorizadas de acesso aos arquivos de sistema;

g) Geração de chaves próprias da AC ou de chaves de usuários finais;

h) Emissão e revogação de certificados;

i) Geração de LCR;

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

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

l) Operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1. Não se aplica.

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

a) Registros de acessos físicos;

b) Manutenção e mudanças na configuração de seus sistemas;

c) Mudanças de pessoal e de perfis qualificados;

d) Relatórios de discrepância e comprometimento; e

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

5.4.1.3. Os registros de auditoria mínimos a serem mantidos pela AC incluem além dos acima:

a) Registros de solicitação, inclusive registros relativos a solicitações rejeitadas;

b) Pedidos de geração de certificado, mesmo que a geração não tenha êxito;

c) Registros de solicitação de emissão de LCR.

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

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

5.4.1.6. A AR vinculada à AC SAFE-ID BRASIL, responsável pela DPC registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos estão obrigatoriamente incluídos em arquivos de auditoria:

a) Os agentes de registro que realizaram as operações;

b) Data e hora das operações;

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

d) A assinatura digital do executante.

5.4.1.6.1. Não se aplica

5.4.1.7. A AC armazena eletronicamente as cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados e dos termos de titularidade.

5.4.2. Frequência de auditoria de registros (*logs*)

A periodicidade de auditoria de registros não é superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da AC. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando-se que não foram alterados. Em seguida procede-se a uma investigação

mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3. Período de Retenção para registros de auditoria

A AC mantém localmente, nas instalações do SERPRO, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 5.5.

5.4.4. Proteção de registro de auditoria

5.4.4.1. Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação.

5.4.4.2. As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação.

5.4.4.3. Os mecanismos de proteção descritos neste item obedece à POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

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

A AC executa procedimentos de backup, de todo o sistema de certificação (sistemas operacionais, aplicação e banco de dados) de duas formas:

a) Diariamente: cópia de segurança; e

b) Semanalmente: cópia armazenada para processos de auditoria.

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

O sistema de coleta de dados de auditoria da AC é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação da AC, pelo sistema de controle de acesso e pelo pessoal operacional. A localização dos recursos se encontra na tabela abaixo:

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de log-in e log-out	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados	Automático	*Software* de AC ou AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado	Automático	*Software* de AR
Logs de *Backup* e restauração	Automático e manual	Sistema operacional e

		pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de *software* e *hardware*	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	*Software* de controle de acesso e pessoal de operações

5.4.7. Notificação de agentes causadores de eventos

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

5.4.8. Avaliações de vulnerabilidade

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

5.5. Arquivamento de Registros

Nos itens seguintes é descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC e pelas ARs vinculadas.

5.5.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC:

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC; e

g) Informações de auditoria previstas no item 5.4.1.

5.5.2. Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:

a) As LCR referentes a certificados de assinatura digital são retidas permanentemente para fins de consulta histórica.

b) Os dossiês dos titulares são retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e

c) As demais informações, inclusive os arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

5.5.3. Proteção de arquivos

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

5.5.4. Procedimentos para cópia de arquivos

5.5.4.1. A primeira cópia é armazenada em servidor de rede apropriado em ambiente nível 4. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo à AC, no site de backup - e recebem 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. É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para datação de registros

Os servidores da AC são sincronizados com a hora fornecida pela AC RAIZ por meio de sua Fonte Confiável do Tempo – FCT conforme DOC-ICP 07 [13]. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.

No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

5.5.6. Sistema de coleta de dados de arquivo

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

Tipo de evento	Sistema de coleção	Registrado por
Solicitações de certificados	Automático e manual	Software de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	Software de AC/ARe pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados	Automático	Software de AC/AR
Emissões de LCR	Automático	Software de AC/AR
Correspondências formais	Manual	Pessoal de operações

5.5.7. Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC e da AR vinculada é verificada na ocasião em que o arquivo é preparado ou diariamente com a execução automática de *script*.

5.6. Troca de chave

5.6.1. A AC comunica os Titulares de Certificado, por e-mail, a necessidade de renovação do certificado, com antecedência de 30 dias, com instruções para a renovação do certificado.

5.6.2. Detalhes dos procedimentos estão descritos nas PC implementadas.

5.7. Comprometimento e Recuperação de Desastre

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

5.7.1. Procedimentos gerenciamento de incidente e comprometimento

5.7.1.1. A AC possui ainda um Plano de Continuidade de Negócio(PCN), de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade de serviços críticos. Possui ainda o Plano de Respostas a Incidentes (PRI) e Plano de Recuperação de Desastres(PRD).

5.7.1.2. Os procedimentos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs, são os seguintes:

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

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

c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários.

d) Documentação dos processos e procedimentos acordados;

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

f) Teste e atualização dos planos.

5.7.2. Recursos computacionais, software e dados corrompidos

A AC possui o Plano de continuidade de Negócio, que contém ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos e que podem ser resumidas no seguinte:

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

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

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

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

5.7.3.1. Certificado de entidade é revogado

A AC possui um PCN que especifica as ações a serem tomadas no caso em que o certificado da AC é revogado, e que podem ser resumidas da seguinte forma:

a) A AC SERPRO, a AC Raiz e os Titulares de Certificados serão notificadas por comunicação segura;

b) A AC revoga os certificados por ela emitidos;

c) A AC solicita um novo certificado;

d) Iniciam-se os procedimentos para emissão dos novos certificados de usuários.

5.7.3.2. Chave de entidade é comprometida

A AC possui um PCN que especifica as ações a serem tomadas no caso de comprometimento de sua chave privada. Após a identificação da crise são notificados os gestores do processo de certificação digital que acionam as equipes envolvidas, para ativar o site de contingência.

5.7.4. Capacidade de continuidade de negócio após desastre

A AC possui um PRD que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC faz parte. Isto significa que o plano deve ter como meta primária, restabelecer A AC para tornar acessível os registros lógicos mantidos dentro do software. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

5.8. Extinção da AC

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

6. Controles Técnicos de Segurança

Nos itens seguintes são definidas as medidas de segurança implantadas pela AC para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. Também são definidos outros controles técnicos de segurança utilizados pela AC e pelas ARs vinculadas na execução de suas funções operacionais.

6.1. Geração e Instalação do Par de chaves

6.1.1. Geração do Par de Chaves

6.1.1.1. O par de chaves da AC é gerado pela própria AC, em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil. Os procedimentos para geração da chave da AC são formalmente descritos e checados no documento da Cerimônia de Geração.

6.1.1.2. Pares de chaves são gerados somente pelo Titular do Certificado correspondente. Os procedimentos específicos estão descritos em cada PC implementada.

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

6.1.1.4. O processo de geração do par de chaves da AC utiliza módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.1.1.6. As chaves privadas da AC foram geradas, armazenadas e utilizadas apenas em hardware criptográfico específico. O módulo criptográfico da AC segue o padrão “Homologação da ICP-Brasil NSH-2”. A utilização de novos módulos é condicionada à homologação junto ao INMETRO conforme legislação da ICP-Brasil vigente.

6.1.2. Entrega da chave privada à entidade

Não se aplica. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. A AC entregará à AC SERPRO cópia de sua chave pública, em formato PKCS#10. Essa entrega será feita por representante legal da AC, em cerimônia específica, em data e hora previamente estabelecida.

6.1.3.2. Chaves públicas são entregues a um solicitante de certificado por meio de uma troca on-line utilizando funções automáticas do software de certificação da AC.

6.1.4. Entrega de chave pública da AC às terceiras partes

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

a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];

b) Página *web* da AC;

c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. As PCs implementadas pela AC definem os tamanhos das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLITICAS 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 seguem o padrão “Homologação da ICP-Brasil NSH-2”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.6.2. A verificação dos parâmetros de geração de chave da AC segue o padrão “Homologação da ICP-Brasil NSH-2”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.1.7.1. Os certificados emitidos pela AC têm no campo “Key usage” (2.5.29.15) ativado os bits digitalSignature, nonRepudiation e keyEncipherment. Os certificados emitidos pela AC são apropriados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal ao uso apenas nas aplicações apresentadas a seguir:

a) Confirmação de Identidade na web;

b) Correio eletrônico;

c) Transações On-Line;

d) Redes privadas virtuais (VPN);

e) Transações eletrônicas;

f) Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Os certificados são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

6.1.7.2. A chave privada da AC é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCRs.

6.2. Proteção da chave privada e controle de engenharia do módulo criptográfico

Nos itens seguintes são definidos os requisitos para a proteção das chaves privadas da AC. Chaves privadas trafegam cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento. Também são definidos os requisitos para a proteção das chaves privadas das ARs vinculadas e das entidades titulares de certificados emitidos pela AC. Cada PC implementada especifica os requisitos específicos aplicáveis.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC adota o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]. O módulo criptográfico da AC segue o padrão “Homologação da ICP-Brasil NSH-3”. Novos módulos são homologados pelo INMETRO conforme estabelecido pela ICP-Brasil.

6.2.1.2. Os módulos de geração de chaves criptográficas dos Titulares de Certificados seguem os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP–

BRASIL [9] no item 3 “Padrões de Harware”. Cada PC implementada pode especificar requisitos adicionais aplicáveis.

6.2.2. Controle “n” de “m” para chave privada

6.2.2.1. A AC implementa o controle múltiplo para a ativação e desativação da sua chave privada através de controles de acesso físico e do software de certificação.

6.2.2.2. É exigido a presença no mínimo de 2 (dois) detentores da chave de ativação (“n”) de um grupo de 15 (quinze) (“m”) para a ativação da chave da AC.

6.2.3. Custódia (*escrow*) de chave privada

Não se aplica.

6.2.4. Cópia de segurança de chave privada

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

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

6.2.4.3. A AC não mantém cópia de segurança da chave privada de Titular de Certificado de assinatura digital.

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

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas de sigilo são arquivadas com um nível de segurança não inferior àquele definido para a chave original. Não são arquivadas chaves privadas de assinatura digital.

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

6.2.6. Inserção de chave privada em módulo criptográfico

A chave privada da AC é inserida no módulo criptográfico de acordo com os procedimentos especificados pelo fornecedor do módulo.

6.2.7. Armazenamento da chave privada em módulos criptográficos

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação da chave privada da AC é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica.

Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

6.2.9. Método de desativação de chave privada

Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

6.2.10. Método de destruição de chave privada

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

A AC armazena as chaves públicas da própria AC e dos titulares de certificados, bem como as LCR emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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

6.3.2.1. A chave privada da AC e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. Cada PC implementada pela AC define o período máximo de validade do certificado que define, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLITICAS DE CERTIFICADO na ICP-Brasil(7).

6.3.2.4. A validade admitida para certificados da AC é limitada à validade do certificado da AC SERPRO. É que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas, implementado pela AC SERPRO.

6.4. Dados de ativação

Nos itens seguintes, estão descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Cada PC implementada deve descrever os requisitos específicos aplicáveis.

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação da chave privada da AC 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, serão únicos e aleatórios.

6.4.2. Proteção dos dados de ativação.

6.4.2.1. Os dados de ativação da AC são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha e são armazenados em ambiente de nível 6 de segurança.

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

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança dos computadores

6.5.1. Requisitos técnicos específicos de segurança computacional

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

6.5.1.2. São requisitos gerais de segurança computacional do equipamento onde serão gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC:

a) Utilização de antivírus, *antitrojan* e *antispyware* instalados, atualizados e habilitados;

b) Utilização de firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades; e

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

Os requisitos específicos aplicáveis são descritos em cada PC implementada.

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

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

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

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

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

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

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

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

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

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

6.5.2. Classificação da segurança computacional

Não disponível.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1. As estações de trabalho da AR, incluindo equipamentos portáteis, recebem as seguintes configurações de segurança:

a) controle de acesso lógico ao sistema operacional;

b) exigência de uso de senhas fortes;

c) diretivas de senha e de bloqueio de conta;

d) logs de auditoria do sistema operacional ativados, registrando:

i. Iniciação e desligamento do sistema;

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

iii. Mudanças na configuração da estação;

iv. Tentativas de acesso(*login*) e de saída do sistema(*logoff*);

v. Tentativas não-autorizadas de acesso aos arquivos de sistema;

vi. Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves;

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

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

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

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

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

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

k) utilização de data e hora de Fonte Confiável do Tempo (FCT).

6.5.3.2. Além dos itens descritos no item 6.5.3.1, as estações de trabalho seguem os requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

6.5.3.3. Não se aplica

6.6. Controles Técnicos do Ciclo de Vida

Nos itens seguintes são descritos os controles implementados pela AC e pelas ARs a ela vinculadas no desenvolvimento de sistemas e no gerenciamento de segurança.

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1. A AC adota o Sistema de Certificação Digital do SERPRO. O ambiente de desenvolvimento segue os padrões e normas formalmente estabelecidas, no mínimo, de acordo com a ISO/IEC 27001:2013. O pessoal de desenvolvimento recebe os treinamentos adequados e passam pelos mesmos critérios de admissão e avaliação periódica da área de produção. A metodologia de desenvolvimento é formalmente aprovada e implementada em software de gestão específico. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluído os testes as versões são disponibilizadas em um ambiente de homologação. Finalizando o processo de homologação das customizações, a gestão avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2. Controle de gerenciamento de segurança

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

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

b) A AC possui ferramenta automatizada para verificar integridade de arquivos e configurações.

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

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

b) Implantação ou modificação de Autoridades Certificadoras com customizações em nível de certificados, páginas *web*, *scripts* etc;

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

d) Instalação de novos serviços na plataforma de processamento.

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na geração da LCR

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

6.7. Controles de Segurança de Rede

6.7.1. Diretrizes Gerais

6.7.1.1 Os controles implementados para garantir a confidencialidade, integridade e disponibilidade dos serviços da AC são os seguintes:

a) Infraestrutura de conectividade, incluindo:

i. Alojamento seguro de equipamento de comunicação;

ii. Firewall seguro e serviços de roteador;

iii. Serviço de LAN seguro; e

iv. Serviço de internet seguro e redundante;

b) Prevenção incidente e avaliação, incluindo:

i. Descoberta de intrusão;

ii. Análise de vulnerabilidade;

iii. Configuração segura de servidor; e

iv. Auditorias técnicas.

c) Administração de infraestrutura, incluindo:

i. Monitoramento de servidor;

ii. Monitoramento de rede;

iii. Monitoramento de URL; e

iv. Relatórios de largura da banda

6.7.1.2. Nos servidores e elementos de infraestrutura e proteção de rede, utilizados pela AC, somente os serviços estritamente necessários são habilitados.

6.7.1.3. Os servidores e elementos de infraestrutura e proteção de rede, tais como, roteadores, *hubs*, *switches*, *firewalls*, localizados no segmento de rede que hospeda o sistema de certificação da AC, estão localizados e operam em ambiente de nível 4.

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

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

6.7.2. *Firewall*

6.7.2.1. Mecanismos de *firewall* estão implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. 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.

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

6.7.3. Sistema de detecção de intrusão (IDS)

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

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

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

6.7.4. Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, *firewall* ou IDS – são registradas em arquivos para análise e são automatizadas. A frequência de exame dos arquivos de registro são diárias ou quando ocorrer algum evento, 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

Nos seguintes itens são descritos os aspectos dos certificados e LCR emitidos pela AC. As Políticas de Certificados abaixo, implementadas pela AC, especificam os formatos dos certificados gerados e das correspondentes LCR. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

PC AC SAFE-ID BRASIL A1	2.16.76.1.2.1.121

7.1. Perfil do Certificado

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

7.1.2. Extensões de certificados

Não se aplica.

7.1.3. Identificadores de algoritmos

Não se aplica.

7.1.4. Formatos de nome

Não se aplica.

7.1.5. Restrições de nome

Não se aplica.

7.1.6. OID (*Object Identifier)* de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil após a conclusão do processo de credenciamento, é **2.16.76.1.1.155**.

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 criticas

Extensões críticas são interpretadas, no âmbito da AC, conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número (s) de versão

As LCR geradas pela AC 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 AC adota as seguintes extensões de LCR:

a) "***Authority Information Access***", **não crítica**: contém somente o método de acesso *id-ad-calssue*r, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação. Não é utilizado nenhum outro método de acesso diferente de *id-ad-calssue*r.

7.2.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

a) "***Authority Key Identifie***r": contém o hash SHA-1 da chave pública da AC que assina a LCR; e

b) "***CRL Number***", **não crítica**: contém um número sequencial para cada LCR emitida.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Não se aplica.

7.3.2. Extensões de OCSP

Não se aplica.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. Frequência e circunstâncias das avaliações

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

Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, a auditoria da AC é realizada pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.4. Tópicos cobertos pela avaliação

8.4.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades da AC estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil e critérios definidos pelo *WebTrust.*

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

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

As ações são tomadas de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

O plano de ações é formalmente definido dentro de ferramenta específica com a definição de responsáveis e prazos.

8.6. Comunicação dos resultados

A comunicação dos resultados é feita de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

Além do ITI, comunicado conforme os procedimentos específicos estabelecidos nos documentos acima, a alta direção e os órgão de governança recebem os relatórios e acompanham o andamento das correções.

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

Valor referente ao serviço de emissão ou renovação de certificados pelas PCs implementadas pela AC e/ou contrato estipulado entre o SERPRO e as entidades que utilizam os serviços da AC.

9.1.2. Tarifas de acesso ao certificado

Não há tarifa que incida sobre este serviço.

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

Valor referente ao serviço de emissão ou renovação de certificados pelas PCs implementadas pela AC e/ou contrato estipulado entre o SERPRO e as entidades que utilizam os serviços da AC.

9.1.4. Tarifas para outros serviços

Não há tarifa que incida sobre este serviço.

9.1.5. Política de reembolso

A AC reembolsará ao solicitante o preço pago pelo certificado no período de validade, exceto em caso de emissão de outro certificado em substituição, sem custos no caso de:

a) Comprometimento da chave privada da AC; e

b) Emissão imprópria ou defeituosa do certificado do solicitante imputável a AC ou à correspondente AR vinculada. (*)

(*) O solicitante deverá solicitar o reembolso ou uma nova emissão à AR emissora do certificado dentro de 10 dias uteis apos a data de aprovação do certificado defeituoso.

9.2. Responsabilidade Financeira

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

9.2.1. Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2. Outros ativos

Conforme regramento desta DPC.

9.2.3. Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3. Confidencialidade da informação do negócio

9.3.1. Escopo de informações confidenciais

9.3.1.1. Todas as informações coletadas, geradas, transmitidas e mantidas pela AC e a AR vinculada são consideradas sigilosas, exceto aquelas informações citadas no item 9.3.2.

9.3.1.2. Como princípio geral, nenhum documento, informação ou registro fornecido à ou AR vinculada deverá ser divulgado.

9.3.2. Informações fora do escopo de informações confidenciais

Os seguintes documentos da AC e AR vinculada são considerados documentos não confidenciais.

a) os certificados e as LCRs emitidas pela AC;

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

c) as PC implementadas pela AC;

d) a DPC da AC;

e) versões públicas de Políticas de Segurança; e

f) a conclusão dos relatórios de auditoria.

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

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

a) As PCs dessa AC;

b) A DPC dessa AC;

c) A Política de Segurança – PS; e

d) A conclusão dos relatórios da auditoria.

9.3.2.3. A AC também divulga, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados emitidos no âmbito da ICP-Brasil.

9.3.3. Responsabilidade em proteger a informação confidencial

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

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

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

9.3.3.4. Não se aplica.

9.4. Privacidade da informação pessoal

9.4.1. Plano de privacidade

A AC assegura 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 é considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

9.4.3. Informações não consideradas privadas

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

9.4.4. Responsabilidade para proteger a informação privadas

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

9.4.5. Aviso e consentimento para usar informações privadas

As informações privadas obtidas pela AC são 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 autorizam a divulgação de seus registros a outras pessoas.

Autorizações formais são 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 é 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 são utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7. Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8. Informações a terceiros

Como diretriz geral nenhum documento, informação ou registro, sob a guarda da AC ou AR vinculada, é fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

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

certificado, analisa, audita e fiscaliza os processos da AR na forma de suas DPCs, PCs e normas complementares.

9.6.1.2. Precisão da informação

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

9.6.1.3. Identificação do requerente

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

9.6.1.4. Consentimento dos titulares

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

9.6.1.5. Serviço

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

9.6.1.6. Revogação

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

9.6.1.7. Existência Legal

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

9.6.2. Declarações e Garantias da AR

Em acordo com item 4 desta DPC.

9.6.3. Declarações e garantias do titular

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

9.6.3.2. A AC informa à AC SERPRO 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:

a) recusarm a utilização do certificado para fins diversos dos previstos nesta DPC;

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

9.6.4.2. O certificado da AC é considerado válido quando:

i. tiver sido emitido pela AC;

ii. não constar como revogado pela AC;

iii. não estiver expirado; e

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

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

9.6.5. Representações e garantias de outros participantes

Não se aplica.

9.7. Isenção de garantias

Não se aplica.

9.8. Limitações de responsabilidades

A AC 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 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.

Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

Não existe responsabilidade da terceira parte perante a AC ou AR, a ela vinculada, que requeira prática de indenização, exceto na hipótese de prática de ato ilícito.

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.

Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. As demais permanecem válidas dentro do escopo de abrangência deste documento.

Nesse caso o corpo técnico da AC examinará a disposição inválida e proporá à Comissão Técnica, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada. As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa DPC serão realizadas por iniciativa da AC por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil.

9.11. Avisos individuais e comunicações com os participantes

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

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC é submetida para AC SERPRO.

9.12.2. Mecanismo de notificação e períodos

Mudança nesta DPC será publicado no site da AC.

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. Também está estabelecido que a DPC da AC não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14. Lei aplicável

A DPC da AC obedece às leis 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 como também as Resoluções do CG da ICP-Brasil. Além disto, é apoiada em uma estrutura contratual entre SERPRO e Titulares de Certificados.

9.15. Conformidade com a Lei aplicável

A AC 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 e AR. Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2. Cessão

Os direitos e obrigações previstos nesta DPC 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	**DOC-ICP-09**
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-08**
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-03**
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	**DOC-ICP-04**
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	**DOC-ICP-02**
[13]	DIRETRIZES PARA SINCRONIZAÇÃO DE FREQUÊNCIA E DE TEMPO NA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS – ICP-BRASIL	**DOC-ICP-07**

10.2. Os documentos abaixo aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sitio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as instruções Normativas que os aprovam.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-Brasil	**DOC-ICP-03.01**
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-Brasil	**DOC-ICP-01.01**
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-Brasil	**DOC-ICP-05.02**
[11]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA DA ICP-Brasil	**DOC-ICP-05.03**

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

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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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

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