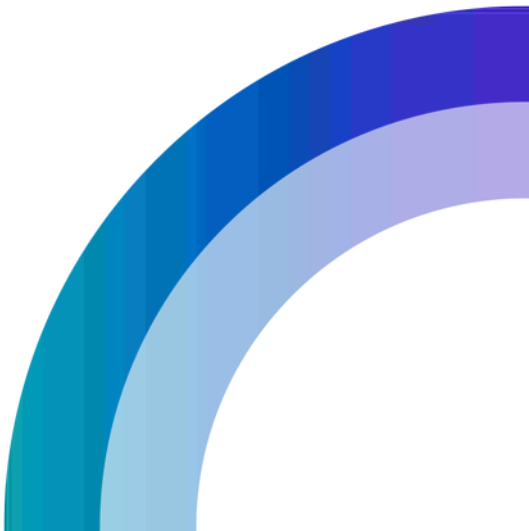
Declaração de Práticas de Certificação
da
Autoridade Certificadora
do
SERPRO

(DPC AC SERPRO)

Versão 9.0 de Setembro 2022



Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Responsável	Motivo	Descrição
6.0	Agosto/2019	Lucia Castelli	Versão Inicial	Atualização dos requisitos Webtrust e consolidação com a versão 4.7, com a simplificação dos processos da ICP-Brasil(Resolução 151);
6.0	Agosto/2019	Osni Bunn	Aprovação	
7.0	Junho/2020	Lucia Castelli	Alterações	Alteração Resolução 155, 164 e167;
7.0	Junho/2020	Alice Vasconcellos	Aprovação	
8.0	Dezembro/2020	Lucia Castelli	Alterações	Alteração conforme Resolução 177
8.0	Dezembro/2020	Alice Vasconcellos	Aprovação	
8.1	Maio/2021	Lucia Castelli	Alterações	Alteração nome do link da crl: http://certificados2.serpro.gov.br/lcr/acserprov4.crl Alteração itens: 4.9.7.1 e 6.3.2.3
8.1	Maio/2021	Alice Vasconcellos	Aprovação	
9.0	Setembro/2022	Fernando Morgado	Alterações	Alterações referentes as resoluções 197 e 204
9.0	Setembro/2022	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 do SERPRO(AC SERPRO), Autoridade Certificadora (AC) integrante da infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na execução dos seus serviços.

1.1.2. A DPC da AC 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. AC 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 do SERPRO”, integrante da ICP-Brasil e comumente referida como “DPC AC SERPRO”. O Identificador de Objeto (OID) desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.2.**

1.2.2. Não se aplica.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

Esta DPC se refere unicamente à Autoridade Certificadora do SERPRO, AC SERPRO, integrante da ICP-Brasil.

1.3.2. Autoridades de Registro

1.3.2.1. A atividade de identificação e cadastramento das ACs de nível imediatamente subsequente ao da AC SERPRO será realizada junto com o processo de credenciamento, não havendo Autoridades de Registro - AR no âmbito da AC SERPRO.

1.3.3. Titulares de Certificado

A AC emite certificados para Autoridades Certificadoras de nível imediatamente subsequente ao seu.

Os titulares dos certificados são as entidades pessoas jurídicas, autorizadas pela AR da AC a receberem certificados digitais emitidos por ela, e credenciadas pela AC Raiz para integrar a ICP-Brasil.

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.

Constituem direitos da terceira parte:

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

b) Verificar a qualquer tempo a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:

i. Não constar da LCR da AC;

ii. Não estiver expirado; e

iii. Puder ser verificado com o uso de certificado válido da AC.

O não exercício desses direitos não afasta a responsabilidade da AC e do titular do certificado.

1.3.5. Outros Participantes

1.3.5.1. A AC utiliza o Serviço Federal de Processamento de dados (SERPRO) como Prestador de Serviço de Suporte – PSS, conforme disponibilizado no endereço: https://ccd.serpro.gov.br/acserpro.

1.4. Usabilidade do Certificado

1.4.1.Uso apropriado do certificado

Os certificados definidos por esta DPC têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR), emitidos pelas ACs de nível imediatamente subsequentes ao da AC.

1.4.2. Uso proibitivo do certificado

Os certificados emitidos pela AC não podem identificar ou verificar qualquer entidade ou assinatura além dos propósitos descritos nesta DPC.

1.5. Política de Administração

Esta DPC é administrada pelo Centro de Certificação Digital do SERPRO (CCD-SERPRO).

1.5.1. Organização Administrativa do documento

Autoridade Certificadora do SERPRO.

1.5.2. Contatos

Administrativo:

Nome: Pedro Moacir Rigo Motta

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

E-mail: certificados@serpro.gov.br

Telefone: (61) 2021-7957

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: Pedro Moacir Rigo Motta

Telefone: (61) 2021-7957

E-mail: certificados@serpro.gov.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
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*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*
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	*National Institute of Standards and Technology*

SIGLA	DESCRIÇÃO
OCSP	*Online Certificate Status Protocol*
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade do Negócio
PIN	Personal Identification Number
PIS	Programa de Integração Social
POP	*Proof of Possession*
PRD	Plano de Recuperação de Desastres
PRI	Plano de Respostas a Incidentes
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSS	Prestadores de Serviço de Suporte
PUK	PIN Unblocking Key
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	*Simple Network Management Protocol*
SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIOS

2.1. Obrigações dos repositórios

2.1.1. Repositórios

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

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

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

2.1.2. 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.

b) Disponibilidade – aquela definida no item 2.2.1;

c) Protocolos de acesso – HTTP e HTTPS;

d) Requisitos de segurança:

i. Os servidores físicos devem estar 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 realização de backup deve ser diária;

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

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

v. Devem realizadas análises periódicas de vulnerabilidades;

vi. A arquitetura segurança para proteção de perímetro deve ser composta por, no mínimo, Firewall, IPS e AntiDDoS;

vii. A monitoração dos eventos de segurança ou indisponibilidade deve ser realiza 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 SERPRO disponibiliza 02(dois) repositórios em infraestruturas de rede segregadas, para distribuição de LCR:

V3	http://ccd.serpro.gov.br/lcr/acserprov3.crl
V4	http://certificados2.serpro.gov.br/lcr/acserprov4.crl http://repositorio.serpro.gov.br/lcr/acserprov4.crl

2.2. Publicação de informações dos certificados

2.2.1. A AC mantém página web, https://ccd.serpro.gov.br/acserpro, com disponibilidade de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana:

2.2.2. As seguintes informações são publicadas na página web da AC:

a) seu próprio certificado;

b) suas LCRs;

c) sua DPC;

d) as PCs que implementam essa AC;

e) Não se aplica;

f) relação, regularmente atualizada, contendo o PSS vinculado.

2.3. Tempo ou Frequência de Publicação

2.3.1. 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

2.4.1. Não há nenhuma restrição ao acesso para consulta a esta DPC, aos certificados emitidos e à LCR da AC.

Acessos para escrita nos locais de armazenamento e publicação serão 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

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

3.1. Atribuição de Nomes

3.1.1. Tipos de nomes

3.1.1.1. As AC de nível imediatamente subsequente ao da AC, titulares de certificados de AC habilitada, terão um nome que as identifique univocamente no âmbito da AC, no padrão ITU X.500.

3.1.1.2. A AC não inclui no certificado das AC subsequentes o nome da pessoa física responsável pelo mesmo.

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 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. Não se aplica.

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

3.1.5. Unicidade de nomes

Os identificadores "*Distinguished Name*" (DN) são únicos para cada titular de certificados no ambito da AC emitente. Números ou letras adicionais podem ser incluídos ao nome 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, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

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 utilizados pela AC SERPRO, responsável 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. Não se aplica

ii. Para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado, e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90(noventa) dias anteriores à data da solicitação.

b) Emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos e biometria apresentados na etapa de identificação e liberação da emissão do certificado no sistema da AC. A extensão Subject Alternative Name é considerada

fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

A etapa “b” do processo de validação de certificado são registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC SERPRO, com a utilização de certificado digital no mínimo do tipo A3. Tais registros serão feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria

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 identidade de uma organização

3.2.2.1. Disposições Gerais

3.2.2.1.1. A confirmação da identidade da pessoa física responsável pela AC de nível imediatamente subsequente ao da AC SERPRO é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

3.2.2.1.2. Os titulares dos certificados são pessoas jurídicas, autorizadas pela AC SERPRO a receberem certificados digitais, credenciadas pela AC Raiz para integrar a ICP-Brasil e habilitadas pela AC SERPRO para emissão de certificados. Será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

3.2.2.1.3. Será 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 elencados no item 3.2.3.1. do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;

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 AC 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 representante legal da AC 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 poderá ser realizado:

a) Mediante comparecimento presencial do responsável pelo certificado;

b) Não se aplica.

3.2.2.2. Documentos para efeitos de identificação de uma organização

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

a) Relativos a sua habilitação jurídica:

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

ii. Se entidade privada:

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

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

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

3.2.2.3. Informações contidas no certificado emitido para uma organização

3.2.2.3.1. Não se aplica.

3.2.2.3.2. Não se aplica.

3.2.2.4. Não se aplica.

3.2.3. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo responsável pela AC de nível imediatamente subsequente ao da AC SERPRO é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

3.2.3.1. Documentos para efeito de identificação de um indivíduo:

As solicitações de certificados, para as AC subordinadas, devem ser realizadas por pessoa física legalmente responsável, que deverá apresentar a seguinte documentação, em sua versão original acompanhada de cópia legível e que permita a identificação do solicitante:

a) Registro de Identidade ou Passaporte, se brasileiro; ou

b) Título de Eleitor, com foto; ou

c) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou

d) Passaporte, se estrangeiro não domiciliado no Brasil;

e) Não se aplica.

f) Não se aplica.

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. Não se aplica.

3.2.3.1.2. Não se aplica.

3.2.3.1.3. Não se aplica.

3.2.3.1.4. Não se aplica.

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7. Não se aplica.

3.2.3.2. Não se aplica.

3.2.4. Informações não verificadas do titular do certificado

Não se aplica.

3.2.5. Validação das autoridades

Na emissão de certificado de AC subsequente é verificado se a pessoa física é o representante legal da AC.

3.2.6. Critérios para interoperação

Não se aplica.

3.2.7. Autenticação da identidade de um equipamento ou aplicação

Não se aplica.

3.2.8. Procedimentos complementares

3.2.8.1. A AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro, como também a fim de cumprir os requisitos da Webtrust para Autoridades Certificadoras[6] disponíveis em http://www.webtrust.org, bem como da norma ISO/IEC 270001:2013.

3.2.8.2. 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 podem ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-Brasil[1].

3.2.8.3.1. Não se aplica.

3.2.8.3.2. Não se aplica

3.2.8.4. Não se aplica.

3.2.8.4.1. Não se aplica.

3.2.8.4.2. Não se aplica.

3.2.9. Procedimentos específicos

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 SERPRO para a geração de novo par de chaves e de seu correspondente novo certificado.

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

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

b) Não se aplica;

c) Não se aplica;

d) Não se aplica;

e) Não se aplica;

f) Não se aplica;

3.3.3. Não se aplica.

3.3.4. Para os casos específicos de expiração ou revogação de um certificado de AC de nível imediatamente subsequente ao da AC SERPRO, responsável pela DPC, este estabelece que, após a

expiração ou revogação de seu certificado, aquela AC deverá executar os processos regulares de geração de seu novo par de chaves.

3.4. Identificação e Autenticação para solicitação de revogação

A solicitação de revogação do certificado à AC Raiz deve ser efetivada pelo preenchimento do FORMULÁRIO DE SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC [8]. Esse formulário deverá ser assinado por seu representante legal. Quando utilizada a versão eletrônica do formulário, ele deve ser assinado digitalmente e enviado à AC Raiz. O formulário pode também ser preenchido em papel, entregue pessoalmente pelo representante à AC Raiz e assinado no ato da entrega.

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

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 3.2.1;

b) Não se aplica;

c) Não se aplica;

d) Não se aplica;

Nota 1 e 2: Não se aplicam.

4.1.1. Quem pode submeter uma solicitação de certificado

4.1.1.1. A solicitação de certificado para AC de nível imediatamente subsequente ao da AC SERPRO somente será possível após o processo de credenciamento e a autorização de funcionamento da AC conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]

4.1.1.2. Não se aplica.

4.1.1.3. Nos casos previstos no item 4.1.1.1, a AC subsequente deverá encaminhar a solicitação de certificado à AC SERPRO por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]

4.1.1.4. A solicitação de um certificado de AC de nível imediatamente subsequente deve ser feita pelos seus representantes legais.

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: AC subordinada, AR e PSS.

4.1.2.1.3. Não se aplica.

4.1.2.2. Obrigações da AC

a) Operar de acordo com DPC da AC;;

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

c) Assegurar a proteção de suas chaves privadas;

d) Notificar a AC Raiz, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação 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 AC de nível imediatamente subsequente ao seu;

h) Informar a emissão do certificado ao respectivo solicitante;

i) Revogar os certificados por ela emitidos;

j) Emitir, gerenciar e publicar suas LCR;

k) Publicar na página *Web* a DPC aprovada que implementa;

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

m) Não se aplica;

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 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 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) Não se aplica;

y) Não se aplica.

4.1.2.3. Responsabilidades da AR

Não se aplica.

4.1.2.4. Obrigações da AR

Não se aplica.

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

A AC executa 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. A AC pode aceitar ou rejeitar pedidos de certificados das AC imediatamente subsequente de acordo com os procedimentos descritos no item 4.1 desta DPC.

4.2.2.2. Não se aplica.

4.2.3. Tempo para processar a solicitação de certificado

A AC deve cumprir os procedimentos determinados na ICP-Brasil. Não haverá tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

4.3.1.1. A emissão de um certificado pela AC é feita em cerimônia específica, com a presença dos representantes da AC, da AC habilitada, de auditores e convidados, na qual são registrados todos os procedimentos executados.

a) AC garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre após a autorização de funcionamento da AC em questão pela AC-Raiz.

b) A AC entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC habilitada.

c) A emissão dos certificados das AC de nível imediatamente subsequente à AC é feita em equipamentos que operam *off-line*.

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

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

O certificado é entregue ao responsável legal ao final da cerimônia de geração.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

A aceitação do certificado se dá no momento em que os dados constantes do mesmo são verificados pela AC ou na primeira utilização da chave privada correspondente.

4.4.1.1. O processo de aceitação de um certificado emitido pela AC SERPRO a uma AC subsequente se dará em duas etapas: na cerimônia de emissão do certificado, perante os representantes legais da mesma, e após sua utilização no ambiente operacional da AC subsequente.

A AC de nível imediatamente subsequente declarará, através de seus representantes legais, mediante assinatura do “Termo de Acordo”, que aceita o certificado emitido. A aceitação implica que o solicitante reconhece a veracidade dos dados contidos no certificado.

4.4.1.2. A aceitação de todo certificado emitido é garantida pela assinatura do Termo de Responsabilidade AC SERPRO pela AC Titular.

4.4.1.3. A não aceitação de um certificado no prazo previsto implica a realização de nova cerimônia, onde é feita a revogação do certificado não aceito e a emissão de novo certificado.

4.4.2. Publicação do certificado pela AC

O certificado da AC SERPRO e os certificados das ACs de nível imediatamente subsequente ao seu 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

Os certificados definidos por esta DPC têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR), emitidos pelas ACs de nível imediatamente subsequentes ao da AC SERPRO.

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

A AC titular deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto na sua própria DPC.

NOTA: Não se aplica.

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

Não se aplica.

4.6.1. Circunstâncias para renovação de certificados

Não se aplica.

4.6.2. Quem pode solicitar a renovação

Não se aplica.

4.6.3. Processamento de requisição para renovação de certificados

Não se aplica.

4.6.4. Notificação para nova emissão de certificado para o titular

Não se aplica.

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

Não se aplica.

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

Não se aplica.

4.7. Nova chave de certificado (Re-key)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica.

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

Não se aplica.

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica.

4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica.

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

Não se aplica.

4.8. Modificação de certificado

Não se aplica.

4.8.1. Circunstâncias para modificação de certificado

Não se aplica.

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6. Publicação de uma modificação de certificado pela AC

Não se aplica.

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

Não se aplica.

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

4.9.1.1. Um certificado de AC de nível imediatamente subsequente ao da AC SERPRO pode ser revogado a qualquer momento por solicitação da AC Titular do Certificado, por decisão da AC SERPRO, do CG da ICP-Brasil ou da AC Raiz.

4.9.1.2. Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

a) Quando constatada emissão imprópria ou defeituosa;

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

c) No caso de dissolução da AC Titular do Certificado;

d) No caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3. Em relação à revogação, deve ainda ser observado que:

a) A AC revogará, 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 determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.9.1.4. Todo certificado deverá ter a sua validade verificada, na respectiva LCR ou OCSP, 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 deverá também ser confirmada por meio das verificações da assinatura da AC SERPRO e do período de validade da LCR.

4.9.2. Quem pode solicitar revogação

A revogação do certificado de uma AC de nível imediatamente subsequente ao da AC SERPRO somente pode ser feita:

a) Por solicitação da AC Titular do Certificado;
b) Por determinação da AC SERPRO;
c) Por determinação do CG da ICP-Brasil ou da AC Raiz;

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. A solicitação de revogação de certificado à AC deve ser efetivada pelo envio do formulário SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC, disponível no site da AC, preenchido pelo representante legal e assinado no ato da entrega, realizada pessoalmente à AC.

4.9.3.2.Como diretrizes gerais, fica estabelecido que:

a) O solicitante da revogação de um certificado deve ser identificado;

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

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

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

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

4.9.3.4. O prazo limite para a conclusão do processo de revogação de certificado de AC subsequente, após o recebimento da respectiva solicitação é de 12 (doze) horas.

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

4.9.3.6. Não se aplica.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1.

4.9.4.2. Não se aplica.

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

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

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

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

A autenticidade da LCR deve também ser 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 AC emite a LCR referente a certificados de AC subordinadas em um prazo máximo de 90 (noventa) dias.

4.9.7.2. Não se aplica.

4.9.7.3. O prazo máximo admitido para a emissão de LCR da AC SERPRO é de 90 (noventa) dias. Em caso de revogação de certificado de AC subordinada, a AC SERPRO emitirá nova LCR no prazo previsto no item 4.9.3.4 e notificar todas as ACs de nível imediatamente subsequente ao seu.

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. Informações de revogação de certificado de AC de nível imediatamente subsequente ao da AC serão divulgadas por meio de página web https://ccd.serpro.gov.br/acserpro

4.9.11.2. Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. No caso do comprometimento da chave privada de uma AC de nível imediatamente subsequente, a mesma deve notificar imediatamente à AC SERPRO, solicitando a revogação de seu certificado.

4.9.12.2. A comunicação à AC deverá ser 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 AC de nível imediatamente subsequente ou 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. Observado o disposto no item sobre descredenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], para a AC SERPRO, responsável por emissão de certificados para Acs subsequentes, o encerramento de suas atividades implicará na revogação do correspondente certificado e o descredenciamento de todas as entidades que estão operacionalmente vinculadas: AC subsequentes e AR vinculada.

As hipóteses para o descredenciamento da AC SERPRO, poderão acontecer quando:

a) Acontecer a expiração do prazo de validade de certificado da AC SERPRO, sem que haja a emissão de novo certificado para substituí-lo;

b) quando do descredenciamento da AC de nível imediatamente superior a AC SERPRO(AC RAIZ);

c) a pedido da própria AC, mediante requerimento, em relação às suas atividades;

d) por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.11.2. Observado o disposto no item sobre descredenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivo são os seguintes:

a) a AC SERPRO comunicará, com 120 (cento e vinte) dias de antecedência, diretamente à AC Raiz e às entidades a ela vinculadas, e publicará em sua página web, para conhecimento

dos titulares de certificados emitidos, a decisão de encerrar suas atividades de emissão de certificados no âmbito da ICP-Brasil ou de não mais emitir certificados para Acs subsequentes; e

b) a AC SERPRO divulgará, pelos 90 (noventa) dias imediatamente anteriores à expiração do certificado, em sua página web, a decisão de encerrar suas atividades no âmbito da ICPBrasil e de não mais emitir certificados para Acs subsequentes, também divulgando sobre a transferência da guarda de seus dados e registro de arquivo.

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 SERPRO pela DPC 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 deverá haver 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 nas instalações de AC

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.

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 podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC. 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: algum tipo de identificação individual, como cartão eletrônico, e a identificação biométrica.

5.1.2.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC, 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. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

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

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

5.1.2.1.11. 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 ambientes de nível 4, e compreende cofres e gabinetes reforçados trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

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

a)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 nas instalações da AC

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 nas instalações da AC

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 nas instalações da AC

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 se aplica.

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 deverá devolver à AC no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC 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 podem ser 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

Na AC existe 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 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 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]. Poderão ser 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 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 poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC, 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;

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 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.

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, suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação, instaurar/solicitar processo administrativo para apurar os fatos e, se for o caso, adotará as medidas legais cabíveis.

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

a) Relato da ocorrência com “*modus operandis*”;

b) Identificação dos envolvidos;

c) Eventuais prejuízos causados;

d) Punições aplicadas, se for o caso; e

e) Conclusões.

5.3.6.3. Concluído o processo administrativo, a AC 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, 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, pelo menos:

a) Esta DPC;

b) Não se aplica;

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. Não se aplica.

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 auditoria de registro será realizada sempre que houver utilização do sistema de certificação.

A periodicidade de auditoria de registros não será 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, em período não superior a uma semana ou sempre que houver utilização do mesmo, seguindo *scripts* previamente desenvolvidos para estas atividades

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

O sistema de coleta de dados de auditoria é interno à AC SERPRO e utiliza processos manuais.

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) As cópias dos documentos para identificação, apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e

c) As demais informações, inclusive os arquivos de auditoria, deverão ser 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 e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	Software de AC e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados	Automático	Software de AC
Emissões de LCR	Automático	Software de AC
Correspondências formais	Manual	Pessoal de operações

5.5.7. Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC SERPRO é verificada:

a) Na ocasião em que o arquivo é preparado;

b) Semestralmente no momento de uma auditoria de segurança programada;

c) Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

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. Não se aplica.

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. Não se aplica.

5.7.2. Recursos computacionais, software e dados corrompidos

A AC possui o Plano de continuidade de Negócio(PCN), 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

5.8.1. A AC SERPRO observa os procedimentos descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

5.8.2. Quando for necessário encerrar as atividades da AC SERPRO, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes. Isto inclui:

a) Prover com maior antecedência possível notificação para:

1. A AC Raiz da ICP-Brasil;

2. Todas as entidades subordinadas.

b) A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC SERPRO;

c) Preservar qualquer registro não transferido a um sucessor;

d) As chaves públicas dos certificados emitidos pela AC SERPRO, 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 SERPRO;

f) A AC SERPRO, 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.

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes são definidas as medidas de segurança implantadas pela AC SERPRO 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 SERPRO 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], usando os padrões transitórios FIPS 140-2 nível 3 para AC SERPRO v3 e v4, e padrão obrigatório ICP-Brasil NSH-3, após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. Pares de chaves são gerados somente pelo titular do certificado correspondente. Os pares de chaves das AC subsequentes são gerados em módulos criptográficos padrão ICP-Brasil NSH-2 ou NSH-3 e FIPS 140-2 nível 3 para AC nas versões v3 e v4.

6.1.1.3. Não se aplica.

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. 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].

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. Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, à AC e fará uso do padrão PKCS#10, em data e hora previamente estabelecidas pela AC-Raiz da ICP-Brasil.

6.1.3.2. Para a entrega de sua chave pública à AC, encarregada da emissão de seu certificado, a AC solicitante faz uso do padrão PKCS#10. Essa entrega é feita por representante legalmente constituído da AC subordinada, em data e hora previamente estabelecida pela AC.

6.1.4. Disponibilização 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) Diretório;

c) Página web da AC: https://ccd.serpro.gov.br/acserpro;

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

6.1.5. Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho das chaves criptográficas associadas a certificados emitidos pela AC será de 4096 (quatro mil e noventa e seis) bits para a AC SERPRO v3 e v4, e de 2048 (dois mil e quarenta e oito) bits para as AC SERPRO v2(expirado), conforme estabelecido para chaves criptográficas associadas a certificados de AC, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.6. Geração de parâmetros de chaves assimétricas e verificação de qualidade dos parâmetros

6.1.6.1 Os parâmetros de geração de chaves assimétricas da AC versões v3 e v4, seguem o padrão “Homologação da ICP-Brasil NSH-3”, 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 versões v3 e v4, seguem o padrão “Homologação da ICP-Brasil NSH-3”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.1.7.1. A chave privada da AC subsequente é utilizada apenas para a assinatura dos certificados por ela emitidos e para assinatura de sua LCR;

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

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 devem trafegar 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 entidades titulares de certificados emitidos pela AC.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC adota o padrão “Homologação da ICP-Brasil NSH-3”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], para certificados na AC SERPRO v2(expirado), v3 e v4(FIPS 140-2 nível 3).

6.2.1.2. O padrão requerido para os módulos de geração de chaves criptográficas das AC de nível imediatamente subsequente ao da AC é o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.2. Controle ‘n de m’ para chave privada

6.2.2.1. A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC é dividida em 15 partes e distribuídas por 15 custodiantes designados pela AC SERPRO (m).

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

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 poderá, a seu critério, manter 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 das chaves privadas das AC de nível imediatamente subsequentes ao seu.

6.2.4.4. A cópia de segurança deve ser 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 das AC subordinadas à AC SERPRO não são arquivadas pela AC SERPRO.

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 de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação da chave privada da AC 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.

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 das ACs subsequentes, 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 uso para as chaves pública e privada

6.3.2.1. A chave privada da AC e das ACs subsequentes, por ela emitidos, será utilizada 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. Não se aplica.

6.3.2.4. A validade admitida para certificados de AC é limitada à validade do certificado da AC SERPRO, desde 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.

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. Não se aplica.

6.4.2. Proteção dos dados de ativação.

6.4.2.1. Os dados de ativação 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. Não se aplica.

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).

6.5.1.3. Os computadores servidores, utilizados pela AC SERPRO e pelas AC subordinadas, 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 ou da AC subordinada, 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 ou AC subsequente. 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 se aplica.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.

6.5.3.2. Não se aplica.

6.5.3.3. Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1. A AC adota o Sistema de Certificação Digital Ywyra, desenvolvido em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluído os testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do CCD 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 opera em equipamento *off-line*, portanto não necessita configuração de segurança de rede.

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. Classificação de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Antes de publicadas, todas as LCR geradas pela AC são 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 (*patch*), 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” (ZDM) - 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 prove 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

7.1. Perfil do Certificado

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 da Versão

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

7.1.2. Extensões de Certificado

A ICP-Brasil define como obrigatórias as seguintes extensões para certificados de AC:

a) "***Authority Key Identifie***r", **não crítica**: o campo *keyIdentifier* contém o *hash* SHA-1 da chave pública da AC SERPRO;

b)**" *Subject Key Identifier***", **não crítica**: contém o *hash* SHA-1 da chave pública da AC titular do certificado;

c) **"*Key Usage"***, **crítica**: somente os bits e *keyCertSign* e *CRLSign* são ativados;

d) "***Certificate Policies***", **não crítica**:

i. o campo *policyIdentifier* contém o OID das PC que a AC titular do certificado implementa;

ii. o campo ***policyQualifiers*** contém o endereço URL da página web, https://ccd.serpro.gov.br/acserpro/docs/dpcacserpro.pdf onde se obtém a DPC da AC SERPRO;

e) O **"*Basic Constraints"***, **crítica**: contém o campo CA=TRUE;

f) **"*CRL Distribution Points" não crítica**:* contém o endereço na Web onde se obtém a LCR correspondente ao certificado:

V3	http://ccd.serpro.gov.br/lcr/acserprov3.crl
V4	http://certificados2.serpro.gov.br/lcr/acserprov4.crl http://repositorio.serpro.gov.br/lcr/acserprov4.crl

7.1.3. Identificadores de Algoritmo

Os certificados emitidos pela AC SERPRO versão - v3 e v4 - são assinados com o uso da suíte de assinatura sha512WithRSAEncryption, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

7.1.4. Formatos de nome

7.1.4.1. Para os certificados emitidos pela AC, o nome da AC titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = Servico Federal de Processamento de Dados – SERPRO

CN = nome da AC

Para os certificados de AC, emitidos pela AC que emitem certificados para o Sistema de Pagamentos Brasileiro – SPB, o nome da AC titular do certificado constante do campo "*Subject*" adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = Servico Federal de Processamento de Dados – SERPRO

OU = CSPB-X onde "X" identifica a AC perante o SPB

CN = nome da AC

7.1.5. Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC são as seguintes:

a) não serão utilizados sinais de acentuação, tremas ou cedilhas;

b) além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caracter e Código	NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D

.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

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 **2.16.76.1.1.2**.

7.1.7. Uso da extensão "*Policy Constraints*"

A extensão "*Policy Constraints*" poderá ser utilizada, da forma definida na RFC 5280, em certificados emitidos pela AC SERPRO para outras ACs.

7.1.8. Sintaxe e semântica dos qualificadores de política

O campo *policyQualifiers* da extensão "*Certificate Policies"* contém o endereço *web* da DPC da AC: https://ccd.serpro.gov.br/acserpro/docs/dpcacserpro.pdf.

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

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

a) "***Authority Key Identifier***", **não crítica**: 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 pela AC

7.3. Perfil de OCSP

Não se aplica.

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

As tarifas previstas pela AC para os serviços prestados às AC de nível imediatamente subsequente ao seu podem ser consultadas através de solicitação via e-mail indicado no item 1.5.2. desta DPC.

9.1.2. Tarifas de acesso ao certificado

As tarifas previstas pela AC para os serviços prestados às AC de nível imediatamente subsequente ao seu podem ser consultadas através de solicitação via e-mail indicado no item 1.5.2. desta DPC.

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

As tarifas previstas pela AC para os serviços prestados às AC de nível imediatamente subsequente ao seu podem ser consultadas através de solicitação via e-mail indicado no item 1.5.2. desta DPC.

9.1.4. Tarifas para outros serviços

As tarifas previstas pela AC para os serviços prestados às AC de nível imediatamente subsequente ao seu podem ser consultadas através de solicitação via e-mail indicado no item 1.5.2. desta DPC.

9.1.5. Política de reembolso

Não há política de reembolso prevista pela AC para os serviços prestados às ACs de nível imediatamente subsequente ao seu.

9.2. Responsabilidade Financeira

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

9.2.1. Cobertura do seguro

Conforme item 4 dessa DPC

9.2.2. Outros ativos

Conforme item 4 dessa DPC

9.2.3. Cobertura de seguros ou garantia para entidades finais

Conforme item 4 dessa 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 SERPRO 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 AC deverá ser divulgado.

9.3.2. Informações fora do escopo de informações confidenciais

Os seguintes documentos da AC 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) Não se aplica;

d) a DPC da AC SERPRO;

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) Não se aplica;

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

9.3.3. Responsabilidade em proteger a informação confidencial

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

9.3.3.2. A chave privada de assinatura digital da AC SERPRO 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. Não se aplica.

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

9.4.3. Informações não consideradas privadas

Informações sobre revogação de certificados de AC de nível imediatamente subsequente ao da AC são fornecidas na LCR.

9.4.4. Responsabilidade para proteger a informação privadas

A AC é responsável 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 poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável.

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

Autorizações formais podem ser apresentadas de duas formas:

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

b) Por meio de pedido escrito com firma reconhecida.

9.4.6. Divulgação em processo judicial ou administrativo

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

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

9.4.7. Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8. Informações a terceiros

Como diretriz geral nenhum documento, informação ou registro, sob a guarda da AC, será 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.

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

Não se aplica.

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, das ACs subsequentes 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 da AC titular de certificado, deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pela AC SERPRO, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

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

9.6.4. Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes devem:

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

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

9.6.4.2. 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 SERPRO 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 deverá ser submetida para AC Raiz.

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. 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**
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	**DOC-ICP-17**
[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**

10.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal.

O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS 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 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for HighVolume Environments, september 2007

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

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

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