COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO- PRODESP

(AC PRODESP SP)

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

VERSÃO 2.0 - 03/10/2022

CONTROLE DE ALTERAÇÕES

Data	*Versão*	*Observações*
13/10/2021	1.0	Redação Inicial
14/03/2022	1.1	Correção do link do repositório da AC
31/08/2022	1.2	Atualização do contato da AC
03/10/2022	2.0	Atualização devido a Resolução nº 204 de 15.09.2022, com relação a senha PIN e PUK

AVISO LEGAL

Copyright © PRODESP Todos os direitos reservados.

PRODESP é uma marca registrada da PRODESP . Todas as restantes marcas, trademarks e service marks são propriedade dos seus respectivos detentores.

É expressamente proibida a reprodução, total ou parcial, do conteúdo deste documento, sem prévia autorização escrita emitida pela PRODESP.

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido a certificacaodigital@sp.gov.br.

Sumário

1. INTRODUÇÃO

1.1. Visão Geral

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

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

1.1.3. Não se aplica.

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

1.1.5 A AC PRODESP SP mantém todas as informações da sua DPC sempre atualizadas.

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

1.2 Nome Do Documento E Identificação

1.2.1. Este documento é designado Declaração de Práticas de Certificação da Autoridade Certificadora PRODESP SP para a emissão de certificados e referida a seguir como "DPC da AC PRODESP SP".

Este documento é identificado pela seguinte informação:

INFORMAÇÃO DO DOCUMENTO	
Versão/Edição	1.1
Data de Aprovação	14/03/2022
Data de Validade	Não aplicável
OID	**2.16.76.1.1.179**
Localização	https://certificadodigital.prodesp.sp.gov.br/media/files/dpc_ac_prodesp_sp.pdf

1.2.2 Não se aplica.

1.3 Participantes Da ICP-Brasil

1.3.1 Autoridades Certificadoras

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

Esta DPC refere-se à Autoridade Certificadora "AC PRODESP SP".

1.3.2 Autoridades de Registro

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

1.3.3 Titulares de Certificado

Os titulares dos certificados emitidos pela AC PRODESP SP são Autoridades Certificadoras de nível imediatamente subsequente ao seu.

1.3.4 Partes Confiáveis

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

1.3.5 Outros Participantes

1.3.5.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC PRODESP SP e/ou por intermédio da sua AR é publicada em

https://certificadodigital.prodesp.sp.gov.br/repositorio/ac/prodespsp

1.4 Usabilidade Do Certificado

1.4.1 Uso Apropriado do certificado

Os certificados emitidos pela AC PRODESP SP têm sua utilização exclusiva para assinatura de certificados digitais de AC de nível imediatamente ao seu e para assinar a sua Lista de Certificados Revogados.

1.4.2 Uso proibitivo do certificado

Não se aplica.

1.5 Política De Administração

1.5.1 Organização administrativa do documento

Nome da AC: AC PRODESP SP

1.5.2 Contatos

Rua da Mooca, 1921 – Mooca – São Paulo, SP

Telefone: (55 11) 0800 0123401

Nome: Certificação Digital

Telefone: (55 11) 2799 9800

Página web: https://www.prodesp.sp.gov.br

E-mail: certificacaodigital@sp.gov.br

1.5.3 Pessoa Que Determina A Adequabilidade Da DPC Com A PC

Nome: Leandro Rocha Carvalho

Telefone: (55 11) 2845-6190

E-mail: certificacaodigital@sp.gov.br

1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

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

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CN	*Common Name*
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
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*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIN	Personal Identification Number
PIS	Programa de Integração Social
PS	Política de Segurança
PSBIO	Prestador de Serviço Biométrico
PSS	Prestadores de Serviço de Suporte
PUK	*PIN Unbloking Key*
RFC	*Request For Comments*
RG	Registro Geral
SNMP	*Simple Network Management Protocol*
UF	Unidade de Federação

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1. As obrigações do repositório da AC PRODESP SP são:

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

2.1.2 O repositório da AC PRODESP SP está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do mês, através de protocolo http, e pode ser encontrado em:

https://certificadodigital.prodesp.sp.gov.br/repositorio/ac/prodespsp

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

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

2.1.4 A AC PRODESP SP deve disponibilizar 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR/OCSP.

http://lcr1.prodesp.sp.gov.br/acprodespsp/acprodespsp.crl

http://lcr2.prodesp.sp.gov.br/acprodespsp/acprodespsp.crl

2.2. Publicação De Informação Dos Certificados

2.2.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC PRODESP SP

http://certificadodigital.prodesp.sp.gov.br/repositorio, obedecendo as regras e os critérios estabelecidos nesta DPC.

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

2.2.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC PRODESP SP

http://certificadodigital.prodesp.sp.gov.br/repositorio, e seu próprio certificado;

a) seu próprio certificado;

b) suas LCR;
c) esta DPC;
d) não se aplica;
e) não se aplica;
f) uma relação, regularmente atualizada, dos PSS e PSBIO vinculados.

2.3. Tempo Ou Frequência De Publicação

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

Os certificados são publicados após emissão.

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

2.4. Controles De Acesso Aos Repositórios

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

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

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Atribuição de Nomes

3.1.1 Tipos de nomes

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

3.1.1.2. Um certificado emitido para uma AC subsequente não inclui o nome da pessoa responsável.

3.1.2 Necessidade de nomes serem significativos

Os certificados emitidos pela AC PRODESP SP exigem o uso de nomes significativos que possibilitam determinar inequivocamente a identidade da organização titular do certificado.

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4 Regras para interpretação de vários tipos de nomes

3.1.4.1 Nomes distintos em certificados são interpretados usando os padrões ITU-T X.501 e a sintaxe ASN.1

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

3.1.5 Unicidade de nomes

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

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

3.1.6 Procedimento para resolver disputa de nomes

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

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

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

3.2 Validação Inicial de Identidade

A AC PRODESP SP realiza a identificação do solicitante ou dos serviços para a emissão de certificado de AC subsequente utilizando-se de meios legais de comunicação ou investigação para a identificação da pessoa física ou jurídica.

3.2.1 Método para comprovar o controle da chave privada

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

3.2.2 Autenticação da identificação da organização

3.2.2.1 Disposições Gerais

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

3.2.2.1.2. Sendo o titular do certificado uma pessoa jurídica, será designada pessoa física como responsável pelo certificado, o representante legal da pessoa jurídica requerente do certificado, ou o procurador constituído na forma do item 3.2. alínea “a”, inciso (ii) acima, o qual será o detentor da chave privada .

3.2.2.1.3. Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.2.2.2;
b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
c) coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e

comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil, bem como os procedimentos para identificação biométrica na ICP-Brasil;e

d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo responsável pelo certificado.

NOTA 01: Não se aplica.

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; ou
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 à sua habilitação jurídica:
   i. Se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e 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. Documento da eleição de seus administradores, quando aplicável;
b) Relativos à sua habilitação fiscal:
   i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
   ii. prova de inscrição no Cadastro Específico do INSS – CEI.

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

3.2.2.3 Informações contidas no certificado emitido para uma organização

Não se aplica.

3.2.2.4 Responsabilidade decorrente do uso do certificado de uma organização

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

3.2.3 Autenticação da identidade de um indivíduo

A AC PRODESP SP realizam a identificação e cadastramento de um indivíduo na ICP-Brasil. Essa confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado ou por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa com base em documentos pessoais de identificação legalmente aceitos e pelo processo biométrico da ICP-Brasil.

3.2.3.1 Procedimento para identificação de um indivíduo

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

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

i. Registro de Identidade, se brasileiro; ou
ii. Título de Eleitor, com foto; ou
iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
iv. Passaporte, se estrangeiro não domiciliado no Brasil.

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

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

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

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

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

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

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

3.2.3.1.4 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.

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

3.2.3.2 Informações contidas no certificado emitido para um indivíduo

Não se aplica.

3.2.3.2.2. Não se aplica.

3.2.3.2.3. Não se aplica..

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

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

3.2.4 Informações não verificadas do titular do certificado
Não se aplica.

3.2.5 Validação das autoridades
Na emissão de certificado de AC subsequente é verificado se a pessoa física é o representante da AC.

3.2.6 Critérios para interoperação
Não se aplica.

3.2.7 Autenticação da identidade de equipamento ou aplicação
3.2.7.1 Disposições gerais

Não se aplica.

3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

Não se aplica.

3.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação

Não se aplica.

3.2.7.4 Autenticação de Identificação de Equipamento para Certificado CF-e-SAT

Não se aplica.

3.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT

Não se aplica.

3.2.7.6 Informações contidas no certificado emitido para um equipamento SAT

Não se aplica.

3.2.7.7Autenticação de Identificação de Equipamento para Certificado OM-BR

Não se aplica.

3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

3.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico

Não se aplica.

3.2.8 Procedimentos Complementares

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

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

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

3.2.8.3.1. Não se aplica.

3.2.8.3.2 Não se aplica.

3.2.8.4 A AC PRODESP SP disponibiliza, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6] e em regulamento editado por instrução normativa da AC Raiz que defina os procedimentos

para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil.

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

3.2.9 Procedimentos específicos
Não se aplica.

3.3 Identificação e autenticação para pedidos de novas chaves
3.3.1.Esta DPC estabelece os processos de identificação do solicitante pela AC PRODESP SP para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração do certificado vigente.

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

a) Adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;
b) A solicitação por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;
c) Não se aplica
d) Não se aplica
e) Não se aplica
f) Não se aplica.

3.3.2.1. Não se aplica.

3.3.3 Não se aplica.

3.3.4 Quando da expiração ou renovação de um certificado de AC de nível imediatamente subsequente ao da AC PRODESP SP, após a expiração ou revogação do certificado, a AC PRODESP SP executará os processos regulares de geração de um novo par de chaves.

3.4 Identificação E Autenticação Para Solicitação De Revogação
A solicitação de revogação de certificado de AC de nível imediatamente subsequente ao da AC PRODESP SP é efetivada através do Formulário de Solicitação de Revogação de Certificado de Autoridade Certificadora Habilitada, preenchido pelo representante legal da AC e assinado no ato de entrega, realizada pessoalmente à AC.

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 do certificado

Os requisitos e procedimentos operacionais estabelecidos pela AC PRODESP SP para as solicitações de emissão de certificado, estão:

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

4.1.1 Quem pode submeter uma solicitação de certificado

A submissão da solicitação deve ser sempre por intermédio da AR.

4.1.1.1 Quando da solicitação de certificado para AC subsequente 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 No casos previstos no item 4.1.1.1 a AC subsequente deverá encaminhar a solicitação de certificado à AC PRODESP SP por meio de seus representantes legais, utilizando o padrão no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9]

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

4.1.2 PROCESSO DE REGISTRO E RESPONSABILIDADES

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

4.1.2.1 Responsabilidades da AC

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

4.1.2.1.2. A AC PRODESP SP responde solidariamente pelos atos das entidades da sua cadeia de certificação: AC subordinada, AR e PSS.

4.1.2.1.3. Não se aplica.

4.1.2.2 Obrigações da AC

As obrigações da AC PRODESP SP são:

a) Operar de acordo com esta DPC;

b) Gerar e gerenciar seus pares de chaves criptográficas;
c) Assegurar a proteção de suas chaves privadas;
d) Notificar a AC Raiz, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
e) Notificar os usuários quando ocorrer suspeita de comprometimento da chave privada da AC PRODESP SP, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) Distribuir seu próprio certificado;
g) Emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu;
h) Informar a emissão do certificado ao respectivo solicitante;
i) Revogar os certificados emitidos;
j) Emitir, gerenciar e publicar sua LCR e quando aplicável, disponibilizar consulta online de situação do certificado (OCSP Online Certifica-te Status Protocole);
k) Publicar em sua página web está DPC da AC PRODESP SP;
l) publicar em sua página web as informações descritas no item 2.2.2 desta DPC;
m) publicar em sua página web informações sobre o descredenciamento de AR;
n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas nesta DPC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil ;
q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
s) manter e testar anualmente seu Plano de Continuidade do Negócio-PCN;
t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-la, de acordo com as normas do CG da ICP-Brasil;
u) informar à terceira parte e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC PRODESP SP;
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) fiscalizar e auditar as AR vinculadas e os prestadores de serviço que lhe sejam vinculados, em conformidade com as políticas, normas e procedimentos da ICP-Brasil; e

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

4.1.2.3 Responsabilidades da AR

A AR é responsável pelos danos a que der causa.

4.1.2.4 Obrigações das AR

As obrigações da AR vinculadas à AC PRODESP SP são:

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar as solicitações de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente da AR hospedado nas instalações da AC PRODESP SP utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil;
d) informar os titulares de certificado a emissão ou a revogação de seus certificados;
e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC PRODESP SP e pela ICP-Brasil, em especial com o contido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da CP-Brasil, bem como Princípios e Critérios Web Trust para AR[5];
f) manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;
g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2;
h) divulgar suas práticas, relativas à cadeia de AC ao qual se vincular, em conformidade com o documento princípios e Critérios Web Trust para AR [5].

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1 Execução das funções de identificação e autenticação

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

4.2.2 Aprovação ou rejeição de pedidos de certificado

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

4.2.3 Tempo para processar a solicitação de certificado

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

4.3 Emissão de Certificado

4.3.1 Ações da AC durante a emissão de um certificado

4.3.1.1. A emissão de certificado pela AC PRODESP SP é realizada em cerimônia especifica com a presença de representante da AC PRODESP SP, da AC credenciada, de auditores e convidados, na qual são registrados todos os procedimentos realizados.

A AC PRODESP SP garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 5 (cinco) dias úteis após a autorização de funcionamento da AC em questão pela AC Raiz.

A AC entrega o certificado emitido para os representantes legais da AC habilitada.

A emissão dos certificados das AC de nível imediatamente subsequente à AC PRODESP SP é feita em equipamentos que operam offline.

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

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

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

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado

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

4.4.1.2. A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado, na primeira utilização da chave privada correspondente.

4.4.1.3. Não se aplica.

4.4.2 Publicação do certificado pela AC

O certificado da AC PRODESP SP é publicado de acordo com o item 2.2 desta DPC.

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

Não se aplica.

4.5 Usabilidade do Par De Chaves e do Certificado

A AC subsequente titular de certificado emitido pela AC deve operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementar, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICPBRASIL [7].

4.5.1. Usabilidade da chave privada e do certificado do titular

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

4.5.1.2 Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos pela AC PRODESP SP são:

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

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

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6 Renovação De Certificados

Em acordo com o item 3.3 desta DPC.

4.6.1 Circunstâncias para renovação de certificados

Em acordo com o item 3.3. desta DPC.

4.6.2 Quem pode solicitar a renovação

Em acordo com o item 3.3. desta DPC.

4.6.3 Processamento de requisição para renovação de certificados

Em acordo com o item 3.3. desta DPC.

4.6.4 Notificação para nova emissão de certificado para o titular

Em acordo com o item 3.3. desta DPC.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com o item 3.3. desta DPC.

4.6.6 Publicação de uma renovação de um certificado pela AC

Não se aplica.

4.6.7 Notificação de emissão de certificado pela AC para outras entidades

Em acordo com o item 4.3. desta DPC.

4.7 Nova Chave De Certificado (Re-Key)

4.7.1 Circunstâncias para nova chave de certificado

Não se aplica.

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

Não se aplica.

4.7.3 Processamento de requisição de novas chaves de certificados

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 atividades

Não se aplica.

4.8 Modificação De Certificado

Não se aplica.

4.8.1 Circunstâncias para modificação de certificado

Não se aplica.

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3 Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4 Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6 Publicação de uma modificação de certificado pela AC

Não se aplica.

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

Não se aplica.

4.9 Suspensão E Revogação De Certificado

4.9.1 Circunstâncias para revogação

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

4.9.1.2. O certificado é obrigatoriamente revogado:

a) quando for constatada emissão imprópria ou defeituosa do mesmo;
b) quando for necessária a alteração de qualquer informação constante no mesmo;
c) no caso de dissolução da AC PRODESP SP;
d) no caso de comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;

4.9.1.3. A DPC observa ainda que:

a) A AC PRODESP SP revoga, no prazo definido no item 4.9.3.3, o certificado da AC titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil.

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

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

4.9.1.4.1. Não se aplica.

4.9.1.4.2. Não se aplica.

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

4.9.2 Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) Por solicitação da AC Titular do Certificado;
b) Por determinação da AC PRODESP SP;
c) Por solicitação da AR PRODESP ;
d) Por determinação do CG da ICP-Brasil;
e) Por determinação da AC Raiz.

4.9.3 Procedimento para solicitação de revogação

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

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

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

4.9.3.2. Como diretrizes gerais:

a) O solicitante da revogação de um certificado é identificado;
b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC PRODESP SP;
c) As justificativas para a revogação de um certificado são documentadas;
d) O processo de revogação de um certificado termina com a geração e a publicação da LCR que contenha o certificado revogado e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC.

4.9.3.3. O prazo máximo admitido para conclusão do processo de revogação do certificado pela AC PRODESP SP, 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 máximo admitido para a conclusão do processo de revogação de certificado da AC PRODESP , após o recebimento da respectiva solicitação, é de 24 (vinte e quatro) horas.

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

4.9.3.6. Não se aplica.

4.9.4 Prazo para solicitação de revogação

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

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

4.9.4.2. Não se aplica.

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

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

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7 Frequência de emissão de LCR

4.9.7.1. Neste item é definida a frequência para a emissão de LCR referente a certificados de AC de nível imediatamente subsequente a AC PRODESP SP.

4.9.7.2. Não se aplica.

4.9.7.3. A frequência máxima admitida para a emissão de LCR referente a certificados de AC Subsequente é de 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente a AC PRODESP SP, é emitida nova LCR no prazo previsto no item 4.9.3.4 e notificada a todas as AC 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 a sua geração.

4.9.9 Disponibilidade para revogação ou 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

Não se aplica.

4.9.12 Requisitos especiais para o caso de comprometimento de chave

Quando houver comprometimento ou suspeita de comprometimento da chave privada, a AC Titular do Certificado deverá comunicar imediatamente a AC PRODESP SP .

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".

4.9.14. Quem pode solicitar suspensão

A AC PRODESP SP, aprovados pelo Comitê Gestor.

4.9.15. Procedimento para solicitação de suspensão

Os procedimentos de solicitação de suspensão serão dados por norma específica da DPC.

4.9.16 Limites no período de suspensão

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

4.10 Serviços de Status de Certificado

4.10.1 Características operacionais

A AC PRODESP SP fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados ou OCSP, conforme item 4.9.

4.10.2 Disponibilidade dos serviços
Ver item 4.9.

4.10.3 Funcionalidades Operacionais
Ver item 4.9.

4.11 Encerramento das Atividades

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

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

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

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

4.12.2 Políticas e práticas de encapsulamento e recuperação de chave de sessão
Não se aplica.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1 Controles Físicos

5.1.1 Construção e localização das instalações da AC

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

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

a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;
b) Instalações para sistemas de telecomunicações;
c) Sistemas de aterramento e de proteção contra descargas atmosféricas;
d) Iluminação de emergência.

5.1.2 Acesso físico

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

5.1.2.1 Níveis de acesso

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

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC PRODESP SP. 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 PRODESP SP transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC PRODESP SP 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 PRODESP SP a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente são utilizados mediante autorização formal e supervisão.

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

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

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

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

5.1.2.1.8. No quarto nível – ou nível 4, interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC PRODESP SP tais como emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível, inclusive o sistema de AR. O nível 4

possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

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

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

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

a) equipamentos de produção on-line e cofre de armazenamento;
b) equipamentos de produção off-line 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, interior aos ambientes de nível 4, compreende um cofre ou um gabinete reforçado trancado. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

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

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

5.1.2.1.14. O sexto nível – ou nível 6, consiste de pequenos depósitos localizados no interior do cofre de Nível 5. Cada um desses depósitos dispõe de 2 fechaduras, sendo uma individual e a outra comum a todos os depósitos. Os dados de ativação da chave privada da AC PRODESP SP são armazenados nesses depósitos.

5.1.2.2.Sistemas físicos de detecção

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

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

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

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

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

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

5.1.2.3 Sistema de controle de acesso

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

5.1.2.4 Mecanismos de emergência

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

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

5.1.3 Energia e ar condicionado

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

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

5.1.3.3. Existem tubulações, dutos, calhas, quadros e caixas – de passagem, distribuição e terminação – projetados e construídos de forma a facilitar vistorias e a detecção de

tentativas de violação. São utilizados dutos separados para os cabos de energia, telefonia e dados.

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

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

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

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

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

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

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

a) gerador de porte compatível;
b) gerador de reserva;
c) sistemas de no-breaks redundantes;
d) sistemas redundantes de ar condicionado.

5.1.4 Exposição à água nas instalações de AC

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

5.1.5 Prevenção e proteção contra incêndio

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

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

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

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

5.1.6 Armazenamento de mídia

A AC PRODESP SP atende às normas NBR 11.515 e NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7 Destruição de lixo

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

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

5.1.8 Instalações de segurança (backup) externas (off-site)

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

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

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

5.2.1.2. A AC PRODESP SP estabelece diferentes perfis para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

O detalhe dos perfis encontra-se em documento interno normativo.

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

5.2.1.4. A AC PRODESP SP possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos seus funcionários. Existe uma lista de revogação com todos os recursos, antes

disponibilizados, que o funcionário devolve à AC PRODESP SP no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

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

5.2.3 Identificação e autenticação para cada perfil

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

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

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

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

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

5.2.4 Funções que requerem separação de deveres

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

5.3 Controles De Pessoal

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

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

b) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

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

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 PRODESP SP e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido, pelo menos, a:

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

5.3.2.2. Não se aplica.

5.3.3 Requisitos de treinamento

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

a) princípios e mecanismos de segurança da AC PRODESP SP e das AR vinculadas;
b) sistema de certificação em uso na AC PRODESP SP;
c) procedimentos de recuperação de desastres e de continuidade do negócio;
d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma dos itens 3.1.9, 3.1.10 e 3.1.11;
e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

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

5.3.5 Frequência e sequência de rodízio de cargos

Não se aplica.

5.3.6 Sanções para ações não autorizadas

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

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

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

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

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

a) advertência;
b) suspensão por prazo determinado;
c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 Requisitos para contratação de pessoal

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

5.3.8 Documentação fornecida ao pessoal

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

a) A DPC da AC PRODESP SP;
b) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
c) Documentação operacional relativa às suas atividades;
d) Contratos, normas e políticas relevantes para as suas atividades.

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

5.4 Procedimentos de Log de Auditoria

5.4.1 Tipos de eventos registrados

5.4.1.1. A AC PRODESP SP registra em arquivos de auditoria todos os eventos relacionados com a segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC PRODESP SP;
c) mudanças na configuração dos sistemas AC PRODESP SP ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não-autorizadas de acesso aos arquivos do sistema;
g) geração de chaves próprias da AC PRODESP SP ou de chaves das AC subsequentes;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
l) operações de escrita nesse repositório, quando aplicável.

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

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

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

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

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

5.4.1.6 A AC PRODESP SP, responsável pela DPC registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) Os agentes de registro que realizaram as operações;
b) Data e hora das operações;
c) A associação entre os agentes que realizaram a validação e aprovação e o certificado gerado; e

d) A assinatura digital do executante.

5.4.1.7. A AC PRODESP SP define, em documento disponível nas auditorias de conformidade, o local de arquivo das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

5.4.2 Frequência de auditoria de registros (logs)

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

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

5.4.3 Período de retenção para registros (logs) de auditoria

A AC PRODESP SP mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 4.6.

5.4.4 Proteção de registro de auditoria

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

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

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

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

Os registros de eventos e sumários de auditoria da AC PRODESP SP têm cópias de segurança semanais, efetuadas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas.

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

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

5.4.7 Notificação de agentes causadores de eventos

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

5.4.8 Avaliações de vulnerabilidade

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

5.5 Arquivamento de Registros

5.5.1 Tipos de registros arquivados

a) solicitações de certificados;
b) solicitações e justificativas de revogação de certificados;
c) notificações de comprometimento de chaves privadas;
d) emissões e revogações de certificados;
e) emissões de LCR;
f) trocas de chaves criptográficas da AC PRODESP SP;
g) informações de auditoria previstas no item 4.5.1.

5.5.2 Período de retenção para arquivo

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;
b) Os dossiês dos titulares deve, 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 retidos por, no mínimo 7 (sete) anos.

5.5.3 Proteção de arquivo

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

5.5.4 Procedimentos para cópia de arquivo

5.5.4.1 A AC PRODESP SP estabelece que uma segunda cópia de todo o material arquivado é armazenada no *site Backup*, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

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

5.5.5 Requisitos para datação de registros

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

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

5.5.6 Sistema de coleta de dados de arquivo (interno e externo)
Todos os sistemas de coleta de dados de arquivo utilizados pela AC PRODESP SP nos seus procedimentos operacionais são automatizados e manuais e internos.

5.5.7 Procedimentos para obter e verificar informação de arquivo
A verificação de informação de arquivo deve ser solicitada formalmente à AC PRODESP SP, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

5.6 Troca de Chave

5.6.1. A AC PRODESP SP fornece novo certificado a AC subsequente utilizando o mesmo procedimento utilizado para emissão do certificado inicial.

A AC PRODESP SP envia uma comunicação ao titular do certificado com 13 (treze) meses de antecedência da data de expiração do mesmo, juntamente com instruções para a solicitação de um novo certificado.

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

5.6.2. Não se aplica.

5.7 Comprometimento e Recuperação de Desastre

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

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

a) As condições para ativar o plano;
b) Procedimentos de emergência;
c) Procedimentos de fallback;
d) Procedimentos de restauração;
e) Cronograma para manutenção do plano;
f) Requisitos de conscientização e educação;
g) Responsabilidades individuais;
h) Objetivo de Tempo de Recuperação (RTO);
i) Testes regulares dos planos de contingência;
j) O plano para manter ou restaurar as operações de negócios da AC PRODESP SP de forma oportuna, após a interrupção ou falha de processos críticos de negócios;
k) Definição de requisitos para armazenar materiais criptográficos críticos em um local alternativo;
l) Definição de interrupções aceitáveis do sistema e um tempo de recuperação;
m) Frequência para realização de cópias de backup;
n) Distância entre as instalações de recuperação e o site principal;

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

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

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;
b) identificação e concordância de todas as responsabilidades e procedimentos de emergência;
c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial é dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;
d) documentação dos processos e procedimentos acordados;
e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
f) teste e atualização dos planos.

5.7.2 Recursos computacionais, software, e/ou dados corrompidos

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

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

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

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado de entidade é revogado

Em caso de revogação do certificado da AC PRODESP SP o Administrador de Segurança, juntamente com o Administrador PKI da AC PRODESP SP, revogará todos os certificados subsequentes.

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

5.7.3.2 Chave da entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC PRODESP SP, o fato é imediatamente comunicado ao Administrador de Segurança que, juntamente com o Administrador PKI da AC PRODESP SP, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade,

será declarada a contingência e a AC PRODESP SP, revogará todos os certificados subsequentes. A AC titular do certificado revogado é informada.

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

5.7.4 Capacidade de continuidade de negócio após desastre

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

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

Caso haja necessidade, as atividades são transferidas para o *site Backup*.

5.8 Extinção da AC

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

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

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 Geração E Instalação do Par de Chaves

6.1.1 Geração do par de chaves

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

6.1.1.2. Pares de chaves das AC subsequente são gerados somente pelas AC subsequente, que indicarão, por seu(s) representante(s) legal(s), a pessoa responsável pela geração do par de chaves criptográficas.

6.1.1.3 A geração do par de chaves de AC Subsequente é realizada em processo verificável, obrigatoriamente na presença de funcionários de confiança da AC Subsequente treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

6.1.1.4 O processo de geração do par de chaves da AC PRODESP SP é feito por hardware.

6.1.1.5. Não se aplica.

6.1.1.6. O módulo criptográfico de geração de chaves assimétricas da AC PRODESP SP adota o padrão obrigatório (com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO – para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.2 Entrega da chave privada à entidade

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

6.1.3 Entrega da chave pública para emissor de certificado

6.1.3.1. A AC PRODESP SP entrega cópia de sua chave pública à AC Raiz em formato PKCS #10. Essa entrega é realizada por representante legal constituído da AC PRODESP SP, em cerimônia específica, em data e hora previamente estabelecida.

6.1.3.2. A chave pública de uma AC Subsequente é entregue ao representante legal da AC Subsequente pela AC PRODESP SP de acordo com procedimentos internamente definidos. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

6.1.4 Disponibilização de chave pública da AC para usuários

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

6.1.5 Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho mínimo das chaves criptográficas associadas aos certificados de AC Subseqüentes é de 4096 bits.

6.1.6 Geração de parâmetros de chaves assimétricas e Verificação da qualidade dos parâmetros

6.1.6.1. Os parâmetros de geração de chaves assimétricas da AC PRODESP SP adotam o padrão definido e regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

6.1.7.1. A chave privada das AC Subsequentes 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 PRODESP SP é utilizada apenas para a assinatura dos certificados por ela emitidos e da sua LCR.

6.2 Proteção da Chave Privada e Controle de Engenharia Do Módulo Criptográfico

A AC PRODESP SP implementa uma combinação de controles físicos, lógicos e procedimentais de forma a garantir a segurança das suas chaves privadas. As chaves privadas da AC PRODESP SP trafegam cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento.

6.2.1 Padrões e controle para módulo criptográfico

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

6.2.1.2. Não se aplica.

6.2.2 Controle “n de m” para chave privada

6.2.2.1. A AC PRODESP SP exige controle múltiplo do tipo “n de m” para utilização da sua chave privada.

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

6.2.3 Custódia (escrow) de chave privada

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

6.2.4 Cópia de segurança de chave privada

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

6.2.4.2. A AC PRODESP SP mantém cópia de segurança de sua chave privada.

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

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo 3DES – 112 bits ou AES – 128 ou 256 bits, conforme 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. Não se aplica.

6.2.5.2. Não se aplica.

6.2.6 Inserção de chave privada em módulo criptográfico

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

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1

6.2.8 Método de ativação de chave privada

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

6.2.9 Método de desativação de chave privada

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

6.2.10 Método de destruição de chave privada

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

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

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

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

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

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

6.3.2.2. Não se aplica.

6.3.2.3. Não se aplica.

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

6.4 Dados de Ativação

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 Geração e instalação dos dados de ativação

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

6.4.1.2. Não se aplica.

6.4.2 Proteção dos dados de ativação

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

6.4.2.2. Os dados de ativação da chave privada da entidade titular do certificado são protegidos contra o uso não autorizado.

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

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

6.5.1.2. A geração do par de chaves das AC subsequentes é realizada em ambiente próprio. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não autorizado.

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

a) controle de acesso aos serviços e perfis da AC PRODESP SP;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC PRODESP SP;
c) uso de criptografia para segurança de base de dados, quando exigido pela classificação das suas informações;
d) geração e armazenamento de registros de auditoria da AC PRODESP SP;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
f) mecanismos para cópias de segurança (backup).

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

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

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

Todos esses eventos são registrados para fins de auditoria.

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

6.5.2 Classificação da segurança computacional

A segurança computacional da AC PRODESP SP segue as recomendações Common Criteria.

6.5.3 Controles de Segurança para as Autoridades de Registro

Não se aplica.

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

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

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

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. A AC PRODESP SP e AR vinculada utilizam ferramentas e procedimentos formais para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

6.6.2.2. A AC PRODESP SP utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação da AC PRODESP SP.

6.6.3 Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração de LCR

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

6.7 Controles De Segurança de Rede

6.7.1 Diretrizes Gerais

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

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

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

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

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

6.7.2 *Firewall*

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

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

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1. O sistema de detecção de intrusão está configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps SNMP*, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta 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 reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento.

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

6.7.4 Registro de acessos não-autorizados à rede

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

6.8 Carimbo do Tempo

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 Perfil do Certificado

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

7.1.1 Número de versão

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

7.1.2 Extensões de certificado

Os certificados emitidos pela AC PRODESP SP obedecem às normas da ICP-Brasil que define como obrigatórias as seguintes extensões:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC PRODESP SP;

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 keyCertSign e CRLSign estão ativados;

d) "Certificate Policies", não crítica:

d.1) o campo policyIdentifier deve conter:

i. os OID das PCs que a AC titular do certificado implementa, se essa AC emite certificados para usuários finais;

d.2) o campo policyQualifiers deve conter o endereço Web da DPC da AC que emite o certificado;

https://certificadodigital.prodesp.sp.gov.br/media/files/dpc_ac_prodesp_sp.pdf

e) "Basic Constraints, crítica: deve conter o campo cA=True;

f) "CRL Distribution Points", não crítica: contém os endereços Web onde se obtém a LCR correspondente:

- http://lcr1.prodesp.sp.gov.br/acprodespsp/acprodespsp.crl
- http://lcr2.prodesp.sp.gov.br/acprodespsp/acprodespsp.crl

7.1.3 Identificadores de algoritmo

Os certificados emitidos pela AC PRODESP SP são assinados utilizando o algoritmo definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.4 Formatos de nome

7.1.4.1 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 = <nome da AC emitente>

CN = <Nome da AC titular>

7.1.5 Restrições de nome

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

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Os acentos devem ser substituídos pelo caractere não acentuado;
- O "ç" deve ser substituído pelo caractere 'c';
- Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	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) da DPC

O OID desta DPC é **2.16.76.1.1.179**

7.1.7 Uso da extensão "Policy Constraints"

Não se aplica.

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 PRODESP SP

http://certificadodigital.prodesp.sp.gov.br/media/files/dpc_ac_prodesp_sp.pdf

7.1.9 Semântica de processamento para extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número (s) de versão

As LCR geradas pela AC PRODESP SP 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 estão descritas todas as extensões de LCR utilizadas e a sua criticidade.

7.2.2.2. A ICP-Brasil define como obrigatórias, e são implementadas pela AC PRODESP SP, as seguintes extensões de LCR:

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

7.3 PERFIL DE OCSP

7.3.1. Número (s) de versão

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

7.3.2. Extensões de OCSP

Em conformidade com a RFC 6960.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 Frequência e Circunstâncias as 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, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

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

8.3 Relação do Avaliador com a Entidade Avaliada

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

8.4 Tópicos Cobertos Pela Avaliação

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

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

8.4.3. As entidades da ICP-Brasil diretamente vinculadas a AC PRODESP SP – AR e PSS, também receberam auditoria prévia, para fins de credenciamento, e a AC PRODESP SP é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

8.5 Ações Tomadas Como Resultado de uma Deficiência

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

8.6 Comunicação dos Resultados

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

9.OUTROS NEGÓCIOS E ASSUNTOS JURIDICOS

9.1 Tarifas de Serviço

9.1.1Tarifas de emissão e renovação de certificados

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

9.1.2 Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

9.1.3 Tarifas de revogação ou de acesso à informação de status

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

9.1.4 Tarifas para outros serviços

Pelos demais serviços será cobrado o valor estabelecido contratualmente.

9.1.5 Política de reembolso

Variável conforme definição interna da PRODESP SP.

9.2 Responsabilidade Financeira

A responsabilidade da AC PRODESP SP é verificada conforme previsto na legislação brasileira.

9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2 Outros Ativos

Conforme regramento desta DPC.

9.2.3. Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3 Confidencialidade da Informação do Negócio

9.3.1 Escopo de informações confidenciais

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

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

9.3.2 Informações fora do escopo de informações confidenciais

Não são consideradas informações sigilosas:

a) os certificados e LCR emitidos pela AC PRODESP SP;
b) informações corporativas ou pessoais que constem no certificados ou em diretórios públicos;
c) esta DPC;
d) versões públicas de Políticas de Segurança;
e) a conclusão dos relatórios de auditoria.

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

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

a) qualquer PC aplicável;
b) qualquer DPC;
c) versões públicas de Política de Segurança – PS; e

d) a conclusão dos relatórios da auditoria.

9.3.2.3. A AC PRODESP SP também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-Brasil.

9.3.3. Responsabilidade em proteger a informação confidencial

9.3.3.1 Os participantes que recebem ou têm 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 AC PRODESP SP gera e mantém sua chave privada, sendo responsável pelo seu sigilo. A divulgação ou utilização indevida da sua chave privada é da sua inteira responsabilidade.

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

9.3.3.4. Não se aplica.

9.4 Privacidade da Informação Pessoal

9.4.1. Plano de privacidade

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

9.4.2. Tratamento de informação como privadas

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

9.4.3. Informações não consideradas privadas

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

9.4.4. Responsabilidade para proteger a informação privada

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

9.4.5. Aviso e consentimento para usar informações privadas

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

9.4.7. Outras circunstâncias de divulgação de informação
Não se aplica.

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

9.5 Direitos de Propriedade Intelectual
De acordo com a legislação vigente.

9.6 Declarações e garantias

9.6.1. Declarações e garantias da AC
A AC declara e garante o quanto segue:

9.6.1.1. Autorização para certificado

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

9.6.1.2 Precisão da Informação

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

9.6.1.3 Identificação do requerente

A AC PRODESP SP implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC PRODESP SP, no

âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos da AR vinculada na forma de suas DPCs e normas complementares.

9.6.1.4 Consentimento dos titulares

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

9.6.1.5 Serviço

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

9.6.1.6 Revogação

A AC PRODESP SP irá revogar certificados da ICP-Brasil por qualquer razão

especificada nas normas da ICP-Brasil.

9.6.1.7 Existência Legal

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

9.6.2. Declarações e garantias da AR

Em acordo com item 4 desta DPC.

9.6.3 Declarações e garantias do titular

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

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

9.6.4 Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes devem:

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

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

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

i. tiver sido emitido pela AC PRODESP SP;
ii. não constar como revogado pela AC PRODESP SP;
iii. não estiver expirado; e
iv. puder ser verificado com 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 PRODESP SP 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 PRODESP SP responde pelos danos que der causa, e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

9.10 Prazo e rescisão

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

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

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

9.11. Avisos individuais e comunicações com os participantes
As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por escrito e entregue à AC PRODESP SP.

9.12 Alterações

9.12.1. Procedimentos para emendas
Qualquer alteração nesta DPC é submetida à aprovação do CG da ICP-Brasil.

9.12.2. Mecanismos de notificação e períodos
Mudança nesta DPC será publicado no site da AC PRODESP SP .

9.12.3. Circunstâncias na qual o OID deve ser alterado
Não se aplica.

9.13 Solução de conflitos

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

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

9.14 Lei aplicável

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

9.15 Conformidade Com A Lei Aplicável

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

9.16.2. Cessão

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

9.16.3. Independência de disposições

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPC não prejudicará as demais disposições, as quais permanecerão plenamente válidas e eficazes.

Neste caso a disposição inválida, nula ou ineficaz será considerada como não escrita, de forma que esta DPC será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.

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

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

10 DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[1]	DIRETRIZES DA POLITICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05

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

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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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

RFC 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.