Declaração de Práticas de Certificação da Autoridade Certificadora

PRODEMGE BR

(AC 1º Nível)

(DPC AC PRODEMGE BR)

Classificação: Pública
Versão 1.0
Junho de 2018

prodemge

Companhia de Tecnologia
da Informação do Estado
de Minas Gerais

CONTROLE DE ALTERAÇÕES E VERSÕES

VERSÃO	DATA	RESOLUÇÃO QUE APROVOU A ALTERAÇÃO	ITEM ALTERADO	DESCRIÇÃO DA ALTERAÇÃO
1.0	07/06/2018	-	-	Versão inicial

SUMÁRIO

LISTA DE ACRÔNIMOS E SIGLAS

Acrônimo e Sigla	Descrição
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CNE	Cadastro Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoa Jurídica
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCI	Política de Classificação de Informação
PCN	Plano de Continuidade de Negócio
PJ	Pessoa Jurídica
POP	Proof of Possession
PS	Política de Segurança
PRD	Plano de Recuperação de Desastres
Prodemge	Companhia de Tecnologia da Informação do Estado de Minas Gerais
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
SAT	Sistema Autenticador e Transmissor

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento descreve as práticas e os procedimentos empregados pela Autoridade Certificadora PRODEMGE BR (AC 1º Nível) - AC PRODEMGE BR, integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, na execução dos seus serviços.

1.1.2. Esta DPC está em conformidade com a estrutura definida no documento do Comitê Gestor da ICP-Brasil REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [1].

1.1.3. A AC PRODEMGE BR está certificada em nível imediatamente subsequente ao da AC Raiz da ICP-Brasil. O certificado da AC PRODEMGE BR contém a chave pública correspondente à sua chave privada, utilizada para assinar os certificados de AC de nível imediatamente subseqüente (AC Subseqüente) ao seu e para assinar a sua Lista de Certificados Revogados (LCR).

1.2. Identificação

Esta DPC é chamada "Declaração de Práticas de Certificação da Autoridade Certificadora PRODEMGE", integrante da ICP-Brasil, e conhecida como "DPC AC PRODEMGE BR". O *Object Identifier* (OID) desta DPC, atribuído pela AC Raiz, após conclusão de seu processo de credenciamento, é **2.16.76.1.1.125**.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades Certificadoras

Esta DPC refere-se, unicamente, à AC PRODEMGE BR integrante da ICP-Brasil e encontra-se publicada em seu endereço *web* https://www.prodemge.gov.br/certificacaodigital.

1.3.2. Autoridades de Registro

1.3.2.1. As Autoridades de Registro (AR) vinculadas à AC PRODEMGE BR, são responsáveis pelo processo de recebimento, validação e encaminhamento de solicitação de emissão ou revogação de certificados digitais e de identificação de seus solicitantes e seus dados estão publicados em seu endereço *web* da AC PRODEMGE BR https://www.prodemge.gov.br/certificacaodigital, conforme itens abaixo:

a) relação de todas as AR credenciadas;

b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;

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

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;

f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC PRODEMGE BR mantém as informações acima sempre atualizadas.

1.3.3. Prestador de Serviços de Suporte

1.3.3.1. A AC PRODEMGE BR publica em seu endereço *web* https://www.prodemge.gov.br/certificacaodigital a relação de todos os seus Prestadores de Serviços de Suporte (PSS).

1.3.3.2. PSS são entidades utilizadas pela AC PRODEMGE BR, ou pelas AR- vinculadas para desempenhar as atividades descritas abaixo:

a) disponibilização de infraestrutura física e lógica;

b) disponibilização de recursos humanos especializados;

c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC PRODEMGE BR manterá as informações acima sempre atualizadas.

1.3.4. Titulares de Certificado

Os certificados emitidos pela AC PRODEMGE BR têm como titulares as AC de nível imediatamente subsequente ao seu.

1.3.5. Aplicabilidade

Os certificados emitidos pela AC PRODEMGE BR têm sua utilização exclusiva para a assinatura de certificados digitais de AC de nível imediatamente subsequente ao seu e de sua Lista de Certificados Revogados (LCR).

1.4. Dados de Contato

Empresa:	Companhia de Tecnologia da Informação do Estado de Minas Gerais - PRODEMGE
Endereço:	Rua da Bahia, 2277 Bairro de Lourdes CEP: 30.160-012 Belo Horizonte - MG
Telefone Fixo:	31 3339-1245
Nome:	Jacira dos Reis Xavier
E-mail geral:	acprodemge@prodemge.gov.br

2. DISPOSIÇÕES GERAIS

2.1. Obrigações e direitos

2.1.1. Obrigações da AC

São obrigações da AC:

a) operar de acordo com a essa DPC;
b) gerar e gerenciar os seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC Raiz, emitente do seu certificado, quando ocorrer o comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
e) notificar as ACs Subsequentes quando ocorrer: suspeita de comprometimento de sua chave privada; emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCRs;
k) publicar em seu endereço *web*, esta DPC da AC PRODEMGE BR
l) publicar em seu endereço *web* as informações definidas no item 2.6.1.2 desse documento;
m) publicar, em seu endereço *web*, informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;
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 Comitê Gestor (CG) da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas nesta DPC, e na Política de Segurança (PS) que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios 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 AC de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
v) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos;
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2. Obrigações da AR

São obrigações da AR:

a) receber solicitação de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado à AC PRODEMGE BR utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [2];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) disponibilizar os certificados emitidos pela AC PRODEMGE BR aos seus respectivos solicitantes;

f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC PRODEMGE BR e pela ICP-Brasil, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [2];
h) manter e garantir a segurança da informação por elas tratadas, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP Brasil;
i) manter e testar anualmente seu PCN;
j) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9 (autenticação da identidade de pessoa física) e 3.1.10 (autenticação da identidade de pessoa jurídica);
k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas

2.1.3. Obrigações do Titular do Certificado

São Obrigações do Titular do Certificado emitido pela AC PRODEMGE BR:
a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, senhas 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 pela DPC da AC PRODEMGE BR e por outros documentos aplicáveis da ICP-Brasil;
e) informar à AC PRODEMGE BR qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

NOTA: Em se tratando de certificado emitido para pessoa jurídica, estas obrigações se aplicam à pessoa física responsável pelo uso do certificado.

2.1.4. Direitos da Terceira Parte (*Relying Party*)

2.1.4.1. Considera-se Terceira Parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

2.1.4.2. Constituem direitos de terceira parte:
a) recusar a utilização do certificado para fins diversos dos previstos por esta DPC
b) verificar, a qualquer tempo, a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
i. não constar da LCR da AC Emitente;
ii. não estiver expirado;
iii. puder ser verificado com o uso de certificado válido da AC Emitente.

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

2.1.5. Obrigações do Repositório

São obrigações do repositório:
a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC PRODEMGE BR e a 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.

2.2. Responsabilidades

2.2.1. Responsabilidade da AC

2.2.1.1. A AC PRODEMGE BR responde pelos danos a que der causa

2.2.1.2. A AC PRODEMGE BR responde, solidariamente, pelos atos das entidades de sua cadeia de certificação: AC subsequentes, AR vinculadas, PSS.

2.2.1.3. Não se aplica.

2.2.2. Responsabilidade da AR

A AR será responsável pelos danos a que der causa.

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (Relying Party)

Não existe responsabilidade da terceira parte (Relying Party), perante a AC PRODEMGE BR que requeira indenização, exceto na hipótese de prática de ato ilícito.

2.3.2. Relações Fiduciárias

A AC PRODEMGE BR indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3. Processos Administrativos

O titular do certificado que sofre perdas e danos decorrentes do uso do certificado digital emitido pela AC PRODEMGE BR tem o direito de comunicar à AC PRODEMGE BR que deseja indenização prevista no item 2.3.2. Para tais casos, são observadas as seguintes condições:

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC PRODEMGE BR, tal comprometimento deve ter sido comprovado através de perícia realizada por especialista independente;

b) nos casos de erro de identificação, o titular do certificado não pode requerer qualquer indenização, quando os dados constantes no certificado corresponderem aos dados fornecidos por esse titular e coletados pela AC PRODEMGE BR;

c) nos casos de erro de transcrição, o titular do certificado não pode requerer qualquer indenização quando houver aceitado o certificado.

2.4. Interpretação e Execução

2.4.1. Legislação

A DPC da AC PRODEMGE BR obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, especialmente a Medida Provisória número 2.200-2 de 24 de agosto de 2001, bem como as resoluções do CG da ICP-Brasil.

2.4.2. Forma de interpretação e notificação

2.4.2.1. Na hipótese de uma ou mais das disposições desta DPC, por qualquer razão, forem consideradas inválidas, ilegais, ou não aplicáveis por lei, somente tais disposições serão afetadas enquanto todas as demais disposições permanecerão válidas dentro do escopo de abrangência deste documento. Nesse caso, o corpo técnico da AC PRODEMGE BR, examinará a disposição invalida e proporá nova redação ou a retirada da disposição afetada.

2.4.2.2. Todas as solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa DPC serão realizadas por iniciativa da AC PRODEMGE BR, por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil e às AC subsequentes se for o caso.

2.4.3. Procedimentos de solução de disputa

2.4.3.1. Esta DPC prevalecerá em caso de conflito entre esse documento e outras declarações, políticas, planos, acordos, contratos ou documentos que a AC PRODEMGE BR adotar.

2.4.3.2. As práticas e os procedimentos descritos nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3.3. Os casos omissos serão encaminhados para apreciação da AC Raiz.

2.5. Tarifas de Serviço

2.5.1 Tarifas de emissão e renovação de certificados

A AC PRODEMGE BR cobrará o valor estabelecido em contrato pela emissão e renovação de certificados.

2.5.2 Tarifas de acesso ao certificado

A AC PRODEMGE BR cobrará o valor estabelecido em contrato pelo acesso ao certificado.

2.5.3 Tarifas de revogação ou de acesso à informação de status

A AC PRODEMGE BR cobrará o valor estabelecido em contrato pela revogação ou acesso à informação de status do certificado.

2.5.4 Tarifas para outros serviços

A AC PRODEMGE BR cobrará o valor estabelecido em contrato para outros serviços.

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

2.6. Publicação e Repositório

2.6.1. Publicação de informação da AC

2.6.1.1. A AC PRODEMGE BR publica e mantém disponível em seu endereço *web* (http://icp-brasil.ac.prodemge.gov.br/repositorio), um repositório com disponibilidade de no mínimo 99,5% (noventa e nove virgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As seguintes informações são publicadas
a) seus próprios certificados;
b) suas LCRs;
c) sua DPC;
d) uma relação, regularmente atualizada, do(s) PSS vinculado(s).

2.6.2. Frequência de publicação

As informações acima serão publicadas sempre que sofrerem alterações.

2.6.3. Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, aos certificados emitidos e à LCR da AC PRODEMGE BR.
Os acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso

incluirão identificação pessoal para acesso aos equipamentos e a utilização de senhas.

2.6.4. Repositórios

Os repositórios da AC PRODEMGE BR podem ser acessados através de seu endereço *web* http://icp-brasil.ac.prodemge.gov.br/repositorio.

2.6.4.1. A AC PRODEMGE BR disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR.

2.7. Fiscalização e Auditoria de Conformidade

2.7.1. 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, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.2. As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu próprio quadro, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [4].

2.7.3. 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 [5].

2.7.4. A AC PRODEMGE BR 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 [5].

2.7.5. A AC PRODEMGE BR é responsável pela realização de auditorias anuais nas entidades a ela vinculadas, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8. Sigilo

2.8.1. Disposições Gerais

2.8.1.1. A chave privada de assinatura digital da AC PRODEMGE BR foi gerada e é mantida pela própria AC PRODEMGE BR, que é responsável pelo seu sigilo. A divulgação ou utilização indevida de sua chave privada de assinatura é de sua inteira responsabilidade.

2.8.1.2. Os titulares de certificados emitidos pela AC PRODEMGE BR, ou os responsáveis pelo seu uso, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1.3. São se aplica.

2.8.2. Tipos de informações sigilosas

2.8.2.1. Todas as informações coletadas, geradas, transmitidas e mantidas pela AC PRODEMGE BR são consideradas sigilosas, exceto as informações citadas no item 2.8.3.

2.8.2.2. Como princípio geral, nenhum documento, informação ou registro fornecido à AC PRODEMGE BR deverá ser divulgado.

2.8.3. Tipos de informações não sigilosas

As informações consideradas não-sigilosas compreendem:

a) os certificados e as LCR emitidos;
b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
c) a DPC da AC;
d) versões públicas de PS;
e) resultado final de auditoria.

2.8.4. Divulgação de informação de revogação ou suspensão de certificado

2.8.4.1. A AC PRODEMGE BR divulga informações de revogação de certificados por ela emitidos, em seu endereço *web* descrita no item 2.6.1 desta DPC, através de sua LCR.

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

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

2.8.5. Quebra de sigilo por motivos legais

A AC PRODEMGE BR apenas fornecerá documentos, informações ou registros sob sua guarda mediante ordem judicial ou por determinação legal.

2.8.6. Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC PRODEMGE BR será fornecido a qualquer pessoa, exceto quando o requerente, por meio de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

2.8.7. Divulgação por solicitação do titular

2.8.7.1. O titular de certificado ou seu representante legal terá amplo acesso a quaisquer de seus próprios dados e identificações e poderá autorizar a divulgação de seus registros a terceiros.

2.8.7.2. Qualquer liberação de informação pela AC PRODEMGE BR, somente será permitida mediante autorização formal do titular do certificado. Autorizações podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado emitido na ICP-Brasil;
b) por solicitação escrita, com firma reconhecida.

2.8.8. Outras circunstâncias de divulgação de informação

Nenhuma outra divulgação de informação sigilosa, que não as expressamente descritas nesta DPC, é permitida.

2.9. Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, e todos os documentos gerados para a AC PRODEMGE BR (eletrônicos ou não), de acordo com a legislação vigente, pertencem e continuarão sendo propriedade da Companhia de Tecnologia da Informação do Estado de Minas Gerais - Prodemge.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Registro Inicial

3.1.1. Disposições Gerais

3.1.1.1. Neste item e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pelas AR vinculadas à AC PRODEMGE BR, responsável para realização dos seguintes processos:

a) Validação da solicitação de certificado – compreendendo as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9 e 3.1.10:

i. confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física / jurídica é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como a sua representante é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo previr expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública, com poderes específicos para atuar perante a ICP-Brasil e com prazo de validade de até 90 (noventa) dias. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim.

ii. confirmação da identidade de uma organização: comprovação de que os documentos apresentados se referem, efetivamente, à pessoa jurídica titular do certificado e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;

iii. emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC PRODEMGE BR;

b) Verificação da solicitação de certificado – Confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:

i. por agente de registro distinto do que executou a etapa de validação;

ii. em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;

iii. somente após o recebimento, na instalação técnica da AR, de cópia da documentação apresentada na etapa de validação;

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

3.1.1.2. Excepcionalmente, o processo de validação poderá ser realizado fora do ambiente físico da AR, através de procedimento de validação externa, mediante o deslocamento do Agente de Registro da AR até o interessado na obtenção do certificado, observadas as hipóteses, a forma e as condições abaixo dispostas, vedada a criação de instalações físicas destinadas a tal fim, qualquer que seja a denominação utilizada, tais como, mas não limitada a, ponto de atendimento, posto de validação, parceiro, canal, agente credenciado ou agência autorizada.

3.1.1.2.1 As AR poderão adotar o procedimento de validação externa nas seguintes hipóteses:

I. Para pessoas com deficiência ou com mobilidade reduzida, conforme definido pela Lei nº 13.146, de 6 de julho de 2015, devidamente comprovado por documento hábil;

II. Para pessoas Politicamente Expostas – PEP, conforme definido na Resolução nº 16, de 28 de março de 2007, do Conselho de Controle de Atividades Financeiras COAF/MF, devidamente comprovado por documento hábil;

III. Para pessoas que se encontrem cumprindo pena ou detidas em estabelecimento prisional;

IV. Para pessoas com incapacidade física momentânea ou por motivo de saúde, em qualquer caso devidamente justificado e comprovado por documento hábil, estejam impedidas ou impossibilitadas de se deslocar até a instalação física da AR;

V. Para atender contratos firmados com entidades públicas cujos os editais de licitação

tenham sido publicados até a data de publicação desta Resolução;

VI. Outras pessoas não citadas anteriormente, mediante solicitação expressa de validação externa pelo titular do certificado, limitado a 15% (quinze por cento) do total de certificados emitidos pela AR no mês imediatamente anterior.

Nota 1: O disposto na alínea VI, aplica-se a partir do mês subsequente à entrada em operação da AR, vedada a validação externa com base no referido dispositivo, no mês do início de sua operação.

Nota 2: Considera-se como total de certificados emitidos pela AR no mês imediatamente anterior, para fins da alínea VI, o volume de certificados emitidos pela AR, informado na documentação encaminhada ao ITI na forma e no prazo previsto pela Instrução Normativa no 14, de 28 de novembro de 2016.

Nota 3: Acaso a AR não tenha emitido certificados no mês anterior ou não tenham sido prestadas as informações na forma ou no prazo exigidos, ficará a AR impossibilitada de emitir novos certificados com fulcro na alínea VI, somente podendo voltar a emiti-los no mês imediatamente subsequente, desde que prestadas as informações de forma tempestiva.

Nota 4: Para o cálculo da quantidade limite disposto na alínea VI, em caso de resultado fracionário, admitir-se-á o arredondamento para a unidade superior.

3.1.1.2.2. A validação externa será realizada no domicílio do titular do certificado digital, nas hipóteses previstas nos incisos I, II e IV, do item 3.1.1.2.1, ou no local que este se encontre, na hipótese do inc. III, do mesmo item.

3.1.1.2.3. Para fins do item anterior, considera-se domicílio do titular do certificado digital, o seu domicílio civil, na forma do disposto no Código Civil, Lei nº 10.406, de 10 de janeiro de2002.

3.1.1.2.4. O local no qual a validação externa será realizada deverá ser informado no Formulário de Validação Externa, a que se refere a alínea “d” do item 3.1.1.2.5. 3.1.1.2.5. A validação fora do ambiente físico da AR deve atender ainda as seguintes condições:

a) utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR;
b) adotar aplicativo de georreferenciamento que permita rastrear o computador móvel utilizado na validação externa, sendo que a localização do equipamento deve ficar disponível no sistema da AR em que o agente de registro deva estar cadastrado previamente;
c) adotar equipamentos de coleta e verificação biométrica do titular e do agente de registro, em atendimento aos padrões da ICP-Brasil;
d) preencher o Formulário de Validação Externa, adendo ADE-ICP-05.D, o qual deverá ser assinado pelo agente de registro e pelo titular do certificado, preferencialmente assinados digitalmente;
e) em se tratando de dossiês físicos do titular de certificado, esses devem ser enviados para a Instalação Técnica em até 5 (cinco) dias úteis;
f) utilização de equipamento específico, destinado exclusivamente para fins de validação externa, vedada a utilização, para tal fim, das estações de trabalho ou outros equipamentos empregados na instalação técnica.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado devem ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC PRODEMGE BR, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3 e possuem validação biométrica do responsável pela execução. Tais registros devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4. 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 no documento

CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [2].

3.1.1.4.1. Não se aplica.

3.1.1.5. Não se aplica.

3.1.1.6. Não se aplica.

3.1.1.7. Não se aplica.

3.1.1.8. Não se aplica.

3.1.1.9. As disposições para a validação de solicitação de certificados para servidores públicos da ativa e militares da União estão contidas no DOC-ICP-05.02.

3.1.1.10. As disposições para validação de solicitação de certificados digitais para titulares pessoa física de conta de depósitos em Bancos Múltiplos e Caixa Econômica Federal autorizados a funcionar pelo Banco Central do Brasil (BACEN) estão contidas no DOC-ICP- 05.02.

3.1.2. Tipos de nomes

3.1.2.1. A AC PRODEMGE BR admite o "D*istinguished Name*" (DN) do padrão ITU X.500 como tipo de nome para os titulares de certificados emitidos, de maneira a identifica-los univocamente.

3.1.2.2. A AC PRODEMGE BR não inclui nos certificados das AC subsequentes o nome da pessoa física responsável pelo mesmo.

3.1.3. Necessidade de nomes significativos

Para identificação dos titulares dos certificados emitidos, a AC PRODEMGE BR faz uso de nomes significativos que possibilitem determinar a identidade da pessoa ou organização a qual está vinculada o certificado.

3.1.4. Regras para interpretação de vários tipos de nomes
Não se aplica.

3.1.5. Unicidade de nomes

O identificador "D*istinguished Name*" (DN) deve ser único e não ambíguo, para cada titular de certificado emitido pela AC PRODEMGE BR. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6. Procedimento para resolver disputa de nomes

A AC PRODEMGE BR reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, a entidade solicitante de certificado deve provar o seu direito de uso de um nome especifico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

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

3.1.8. Método para comprovar a posse de chave privada

A confirmação de que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, item 2.3, relativos ao Proof of Possession (POP).

3.1.9. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

3.1.9.1 Documentos para efeito de identificação de um indivíduo

Deve ser apresentada a seguinte documentação, em sua versão original e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado:

a) Cédula de Identidade ou Passaporte, se brasileiro;
b) Carteira Nacional de Estrangeiro (CNE), se estrangeiro domiciliado no Brasil;
c) Passaporte, se estrangeiro não domiciliado no Brasil;
d) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses até data da validação presencial;
e) Mais um Documento oficial com fotografia, no caso de certificados de tipos A4 e S4;
f) Fotografia da face do requerente, de um certificado digital ICP-Brasil, conforme disposto no documento PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL [3];
g) Impressões digitais do requerente, de um certificado digital ICP-Brasil, conforme disposto no documento PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL [3].

Nota 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

Nota 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

Nota 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

Nota 4: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a Carteira Nacional de Habilitação (CNH) ou o Passaporte Brasileiro.

Nota 5: Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [2].

Nota 6: Caso haja divergência dos dados constantes do documento de identidade, a solicitação de emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

Os documentos que possuem data de validade precisam estar dentro do prazo, à exceção da CNH que permanece válida como documento de identificação mesmo que sua data de validade esteja expirada.

3.1.9.2. Informações contidas no certificado, emitido para um indivíduo

3.1.9.2.1. Não se aplica.

3.1.9.2.2. Não se aplica.

3.1.9.2.3. Não se aplica.

3.1.10. Autenticação da identidade de uma organização

3.1.10.1 Disposições Gerais

3.1.10.1.1. Os procedimentos empregados pelas AR vinculadas para a confirmação da identidade de uma pessoa jurídica são feitos mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

3.1.10.1.2. Sendo titular do certificado pessoa jurídica, será designado pessoa física, como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente e preferencialmente será designado como responsável pelo certificado um dos representantes legais da pessoa jurídica.

3.1.10.1.3. Será feita a confirmação da identidade da organização e das pessoas físicas que as representam nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.1.10.2;

b) apresentação do rol de documentos elencados no item 3.1.9.1 dos representantes legais da pessoa jurídica e do responsável pelo uso do certificado;

c) presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do TERMO DE TITULARIDADE DE CERTIFICADO DIGITAL DE AC SUBSEQUENTE de que trata o item 4.1.1.

3.1.10.2. 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 Cadastro Nacional de Pessoa Jurídicas (CNPJ);

ii. se entidade privada:

1 - ato constitutivo, devidamente registrado no órgão competente;

2 - documentos da eleição de seus administradores, quando aplicável;

b) relativos à sua habilitação fiscal:

i. prova de inscrição no CNPJ; ou

ii. prova de inscrição no Cadastro Específico do INSS (CEI).

Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.10.3.1. Não se aplica.

3.1.10.3.2. Não se aplica.

3.1.11 Autenticação da identidade de um equipamento ou uma aplicação

3.1.11.1. Disposições Gerais

3.1.11.1.1. Não se aplica.

3.1.11.1.2. Não se aplica.

3.1.11.1.3. Não se aplica.

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

3.1.11.2.1. Não se aplica.

3.1.11.2.2. Não se aplica.

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

3.1.11.3.1. Não se aplica.

3.1.11.3.2. Não se aplica.

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

3.1.12.1. Disposições Gerais

3.1.12.1.1. Não se aplica.

3.1.12.1.2. Não se aplica.

3.1.12.1.3. Não se aplica.

3.1.12.2. Procedimentos para efeito de identificação de um equipamento SAT

3.1.12.2.1. Não se aplica.

3.1.12.3. Informações contidas no certificado emitido para equipamento SAT

3.1.12.3.1. Não se aplica.

3.1.12.3.2. Não se aplica

3.2. Geração de novo par de chaves antes da expiração do atual

3.2.1. Antes da expiração do certificado vigente, o processo de identificação do solicitante utilizado pela AC PRODEMGE BR para geração de novo par de chaves, e de seu correspondente certificado, será o mesmo da primeira emissão.

3.2.2. Esse processo será conduzido através da adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado.

3.2.3. Não se aplica.

3.3. Geração de novo par de chaves após expiração ou revogação

3.3.1**.** Após a revogação ou expiração do certificado, os procedimentos utilizados para a confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo descritos nesta DPC.

3.3.2. Após a expiração ou revogação de um certificado de AC de nível subsequente ao da AC PRODEMGE BR, deverão ser executados os processos regulares de geração de seu novo par de chaves.

3.4. Solicitação de Revogação

Somente os agentes elencados no item 4.4.2 podem solicitar a revogação de um certificado. O procedimento para solicitação de revogação do certificado está descrito no item 4.4.3. As solicitações de revogação de certificado são, obrigatoriamente, documentadas.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado

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

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.1;

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

c) um termo de titularidade assinado pelo titular do certificado e pelo responsável pelo uso do certificado, conforme adendo referente ao TERMO DE TITULARIDADE – PESSOA JURÍDICA [6] específico.

4.1.2. A solicitação de certificado para uma AC de nível imediatamente subsequente ao da AC PRODEMGE BR, somente é possível após o deferimento do processo de credenciamento e a autorização de funcionamento da AC solicitante pela AC Raiz, conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7].

4.1.3. A solicitação de certificado para equipamento de carimbo de tempo de Autoridade de Carimbo de Tempo (ACT) credenciada na ICP-Brasil somente será possível após o deferimento do processo de credenciamento e a autorização de funcionamento da referida ACT, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7]

4.1.4. Nos casos previstos no item 4.1.2, a AC subsequente deve encaminhar a solicitação de certificado à AC PRODEMGE BR por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8].

4.2 Emissão de Certificado

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

a) AC PRODEMGE BR garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorrem em, no máximo, 10 (dez) dias úteis após a autorização de funcionamento da AC em questão pela AC RAIZ.

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

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

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

4.3. Aceitação de Certificado

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

4.3.2. A AC de nível imediatamente subsequente irá declarar, através de seus representantes legais, mediante assinatura do TERMO DE ACEITAÇÃO DE CERTIFICADO DIGITAL DE AC SUBSEQUENTE, que aceita o certificado emitido. A aceitação implica que o solicitante reconhece a veracidade dos dados contidos no certificado.

4.3.3**.** O certificado é considerado definitivamente aceito assim que for utilizado para uma de suas finalidades.

4.4. Suspensão e Revogação de Certificado

4.4.1. Circunstâncias para revogação

4.4.1.1. A revogação de um certificado emitido pela AC PRODEMGE BR pode ser solicitada, a qualquer tempo, pelos agentes elencados no item 4.4.2 desta DPC.

4.4.1.2. Um certificado deve ser obrigatoriamente revogado pelos seguintes motivos:

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

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

a) A AC PRODEMGE BR revoga, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil e;
b) CG da ICP-Brasil ou a AC Raiz determina a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.4.2. Quem pode solicitar revogação

A solicitação para a revogação do certificado de uma AC de nível imediatamente subsequente ao da AC PRODEMGE BR somente pode ser realizada por:

a) AC titular do certificado;
b) AC PRODEMGE BR;
c) Determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. A solicitação de revogação de certificado deverá ser feita através de formulário específico permitindo a identificação inequívoca do solicitante. Os agentes habilitados, conforme o item 4.4.2, podem facilmente a qualquer tempo solicitar a revogação do certificado.

4.4.3.2. Como diretriz geral fica estabelecido que:

a) o solicitante da revogação de um certificado será identificado;
b) as solicitações de revogação, e ações delas decorrentes, serão registradas e armazenadas;
c) as justificativas para a revogação de um certificado serão documentadas;
d) o processo de revogação de um certificado terminará, com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.4.3.3. Não se aplica.

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

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

4.4.3.6. Não se aplica.

4.4.4. Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1 desta DPC. A AC subsequente poderá solicitar a revogação de seu certificado em nova emissão sem ônus no período correspondente entre a emissão e a aceitação

definitiva do mesmo definidos no item 4.3.

4.4.4.2. Não se aplica.

4.4.5. Circunstâncias para suspensão

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

4.4.6. Quem pode solicitar suspensão

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

4.4.7. Procedimento para solicitação de suspensão

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

4.4.8. Limites no período de suspensão

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

4.4.9. Frequência de emissão de LCR

4.4.9.1. A frequência máxima admitida, para a emissão de LCR pela AC PRODEMGE BR, referente a certificados de AC subsequentes é de 45 (quarenta e cinco) dias.

4.4.9.2. Não se aplica.

4.4.9.3. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC PRODEMGE BR emitirá nova LCR no prazo previsto no item 4.4.3.4 e notificará todas as AC de nível imediatamente subsequente ao seu.

4.4.9.4. Não se aplica.

4.4.10. Requisitos para verificação de LCR

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

4.4.10.2. A autenticidade da LCR deverá também ser confirmada por meio da verificação da assinatura da AC emitente e do período de validade da LCR.

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

A AC PRODEMGE BR não disponibiliza diretório online ou um servidor de *Online Certificate Status Protocol* (OCSP) para verificar o estado dos certificados emitidos pela AC PRODEMGE BR.

4.4.12. Requisitos para verificação de revogação *on-line*

A AC PRODEMGE BR não disponibiliza diretório online ou um servidor de OCSP para verificar o estado dos certificados emitidos pela AC PRODEMGE BR.

4.4.13. Outras formas disponíveis para divulgação de revogação

Não se aplica.

4.4.14. Requisitos para verificação de outras formas de divulgação de revogação

Não se aplica.

4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. Quando houver comprometimento da chave privada de um certificado emitido pela AC PRODEMGE BR, o titular deverá notificar imediatamente à AC PRODEMGE BR, solicitando a revogação de seu certificado, conforme item 4.4.3 desta DPC.
4.4.15.2. A AC PRODEMGE BR deverá ser comunicada do comprometimento ou suspeita de comprometimento da chave privada através de formulário específico permitindo a identificação inequívoca do solicitante.

4.5. Procedimentos de Auditoria de Segurança

4.5.1. Tipos de eventos registrados

4.5.1.1. A AC PRODEMGE BR registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivo 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 PRODEMGE BR;
c) Mudanças na configuração da AC PRODEMGE BR ou nas suas chaves;
d) Mudanças nas políticas de criação de certificados;
e) Tentativas de acesso (*login*) e de saída do sistema (*logoff*);
f) Tentativas não autorizadas de acesso aos arquivos de sistema;
g) Geração de chaves próprias da AC PRODEMGE BR ou de chaves de 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;
l) Operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A AC PRODEMGE BR registra 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.

4.5.1.3. As informações registradas pela AC PRODEMGE BR estão descritas nos itens acima.

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

4.5.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC PRODEMGE BR é armazenada, eletrônica ou manualmente, em local único, conforme o documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9].

4.5.1.6. Não se aplica.

4.5.1.7. A AC PRODEMGE BR define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos, utilizados para identificação apresentados no momento da solicitação e revogação de certificados, e dos termos de titularidade.

4.5.2. Frequência de auditoria de registros (logs)

A periodicidade de auditoria de registros não é superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da AC PRODEMGE BR. Todos os eventos

significativos são explicados em relatório de auditoria de registros. Tal análise contempla uma inspeção breve de todos os registros verificando-se que não foram alterados, em seguida procede-se a uma investigação detalhada de todos os alertas e/ou irregularidades identificadas nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3. Período de retenção para registros (*logs*) de auditoria

A AC PRODEMGE BR mantém localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4. Proteção de registro (log) de auditoria

4.5.4.1. 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 operacionais.

4.5.4.2. Informações manuais de auditoria são protegidos contra leitura não autorizada, modificação e remoção através de controles aos ambientes físicos onde são armazenados estes registros.

4.5.4.3. Os mecanismos de proteção descritos obedecem à POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9]

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

A AC PRODEMGE BR executa, automaticamente pelo sistema ou manualmente pelos administradores do sistema, o procedimento de backup dos registros de auditoria semanalmente.

4.5.6. Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é interno à AC PRODEMGE BR e é uma combinação de processos manuais e automatizados, executada por seu pessoal operacional ou por seus sistemas.

4.5.7. Notificação de agentes causadores de eventos

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

4.5.8. Avaliações de vulnerabilidade

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

4.6. Arquivamento de Registros

4.6.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC PRODEMGE BR:

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

4.6.2. Período de retenção para arquivo

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

a) as LCR e os certificados de assinatura digital são retidas permanentemente para fins

de consulta histórica;
b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade são retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. As prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado;
c) as demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

4.6.3. Proteção de arquivo

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme o documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9].

4.6.4. Procedimentos para cópia de segurança (*backup*) de arquivo

4.6.4.1. A AC PRODEMGE BR estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC PRODEMGE BR e recebem o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

4.6.4.3. É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.6.5. Requisitos para datação de registros

Os servidores da AC PRODEMGE BR são sincronizados com a hora fornecida pela AC RAIZ por meio de sua Fonte Confiável do Tempo – FCT conforme DOC-ICP 07 [10]. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos. No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.6. Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela AC PRODEMGE BR em seus procedimentos operacionais são internos.

4.6.7. Procedimentos para obter e verificar informação de arquivo

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

4.7. Troca de chave

4.7.1. A AC PRODEMGE BR comunicará à AC subsequente, com 90 (noventa) dias de antecedência, o vencimento do seu certificado, incluindo neste comunicado as informações necessárias para a solicitação de uma nova chave.

4.7.2. Não se aplica.

4.8. Comprometimento e Recuperação de Desastre

Os requisitos relacionados aos procedimentos de notificação e recuperação de desastres estão descritos no PCN da AC PRODEMGE BR, estabelecido conforme o documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL[9], para garantir a continuidade de seus serviços críticos.

4.8.1. Recursos computacionais, software, e dados corrompidos

Procedimentos descritos no PCN da AC PRODEMGE BR.

4.8.2. Certificado de entidade é revogado

Procedimentos descritos no PCN da AC PRODEMGE BR.

4.8.3. Chave de entidade é comprometida

Procedimentos descritos no PCN da AC PRODEMGE BR.

4.8.4. Segurança dos recursos após desastre natural ou de outra natureza

Procedimentos descritos no PCN da AC PRODEMGE BR.

4.8.5. Atividades da Autoridade de Registro
Não se aplica.

4.9. Extinção dos serviços de AC, AR ou PSS

4.9.1. A AC PRODEMGE BR observa os procedimentos descritos no item 4 do –documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP BRASIL [7].

4.9.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC PRODEMGE BR segue os requisitos e procedimentos descritos no documento **Plano de Encerramento**. Esse plano tem abordagem multidisciplinar envolvendo aspectos de várias áreas da companhia, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC PRODEMGE BR:

a) comunicará publicamente a extinção dos serviços da AC PRODEMGE BR, através de publicação em jornal de grande circulação.
b) revogará todos os certificados gerados pela AC PRODEMGE BR nos prazos estipulados nesta DPC após a publicação e comunicará às partes afetadas através de mensagem eletrônica.
c) extinguirá os serviços de emissão de certificados.
d) extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços de status *on-line* após a revogação completa de todos os certificados.
e) destruirá a chave privada da AC PRODEMGE BR extinta seguindo o procedimento descrito na DPC Item 6.2.9.
f) transferirá os dados e gravações da AC PRODEMGE BR para a Autoridade Certificadora sucessora, aprovada pela AC Raiz. O período no qual os mesmos ficarão armazenados está descrito na DPC item 4.6.
g) transferirá as chaves públicas dos certificados emitidos pela AC PRODEMGE BR para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC PRODEMGE BR. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.
h) o responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC PRODEMGE BR.
i) transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

No caso de encerramento das atividades como AR vinculada a AC PRODEMGE BR, a AR deverá seguir os seguintes requisitos e procedimentos

a) comunicará publicamente a extinção dos serviços de AR vinculada AC PRODEMGE BR, através de publicação em jornal de grande circulação.
b) extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados;
c) ficará responsável pela guarda dos documentos, dados e registros relativos aos pedidos

de emissão de certificados para a AC PRODEMGE BR, devendo fornecê-los sempre que solicitada pelo Titular, ou pela AC PRODEMGE BR. O período no qual os mesmos ficarão armazenados está descrito na DPC item 4.6.

Em caso de falência ou extinção da AR a documentação e registros relativos à emissão de certificados deverá ser entregue para guarda da AC PRODEMGE BR.

No caso de encerramento das atividades como PSS vinculada a AC PRODEMGE BR, a AC PRODEMGE BR, diretamente ou por intermédio da AR, deverá seguir os seguintes requisitos e procedimentos:

a) publicará, em seu endereço *web*, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso;

b) manterá a guarda de toda a documentação comprobatória em seu poder.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

5.1. Controles Físicos

5.1.1. Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação da AC PRODEMGE BR 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. Todos os aspectos de construção das instalações da AC PRODEMGE BR, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos abaixo:

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

5.1.2. Acesso físico nas instalações da AC

O acesso físico às dependências da AC PRODEMGE BR é gerenciado e controlado internamente conforme POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9].

5.1.2.1. Níveis de Acesso

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

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

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão os equipamentos utilizados na operação da AC PRODEMGE BR, em nível superior ao Nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, dispositivos eletrônicos inteligentes portáteis têm entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

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

5.1.2.1.5. O **Terceiro Nível** – ou **Nível 3** – é interno ao segundo nível e será o primeiro nível a abrigar material e atividades sensíveis da operação da AC PRODEMGE BR. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não tem permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por, no mínimo, um empregado 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: a identificação individual, através de um cartão eletrônico e a identificação biométrica,

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

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

5.1.2.1.9. No quarto nível, todas as paredes, 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, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esse ambiente de nível 4, que constitui a chamada sala-cofre principal, tem proteção contra interferência eletromagnética externa.

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

5.1.2.1.11. Na AC PRODEMGE BR, existe 1 (um) ambiente de quarto nível que abriga e segrega:

a) equipamentos de produção on-line e cofre de armazenamento;
b) equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores;
c) equipamentos de produção off-line e cofre de armazenamento.

5.1.2.1.12. O **Quinto Nível** – ou **Nível 5** - é interno ao quarto nível, sendo composto por um cofre reforçado e trancado. Materiais criptográficos, tais como, chaves, dados de ativação e suas cópias e equipamentos criptográficos são armazenados neste ambiente.

5.1.2.1.13. Para elevar o nível de segurança do material armazenado, o cofre obedece às seguintes especificações mínimas:

a) construído em aço;
b) possui tranca com chave.

5.1.2.1.14 O **Sexto Nível** – ou **Nível 6** – consiste de pequenos depósitos localizados no interior do Quinto Nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação de ativação da AC PRODEMGE BR estão armazenados em um desses depósitos.

5.1.2.2. Sistemas Físicos de Detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 1 (um) ano. Elas são testadas (verificação de trechos aleatórios no início, meio e no final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas estão armazenadas no 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, permanentemente, por sistema de notificação de alarmes. A partir do nível 2, vidros que separam níveis de acesso, possuem um mecanismo adicional de alarme de quebra de vidros, que está ligado, também ininterruptamente.

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

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

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

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

5.1.2.4. Mecanismos de emergência

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

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

5.1.3. Energia e ar condicionado nas instalações da AC

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

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

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

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

5.1.3.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9]. Qualquer modificação nessa rede é previamente documentada.

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

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

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização é

permanentemente monitorada pelo sistema de notificação de alarmes.

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

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

a) geradores de capacidade superior à demanda;
b) geradores de reserva;
c) sistema 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, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5. Prevenção e proteção contra incêndio nas instalações de AC

5.1.5.1. Os sistemas de prevenção contra incêndios da AC PRODEMGE BR possuem alarmes preventivos, antes da fumaça visível, que são disparados 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 PRODEMGE BR 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 se abre quando a porta do nível anterior estiver fechada.

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

5.1.6. Armazenamento de mídia nas instalações de AC

A AC PRODEMGE BR atende a Norma Brasileira - NBR 11.515/NB 1334 – CRITÉRIOS DE SEGURANÇA FÍSICA RELATIVOS AO ARMAZENAMENTO DE DADOS.

5.1.7. Destruição de lixo nas instalações de AC

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

5.1.7.2. Serão fisicamente destruídos todos os dispositivos eletrônicos não mais utilizáveis, e que em algum momento foram utilizados para o armazenamento de informações sensíveis.

5.1.8. Instalações de segurança (*backup*) externas (*off-site*) para AC

As instalações de segurança (*backup*) atende aos requisitos mínimos estabelecidos por esta DPC. A sua localização é tal que, em caso de sinistro que tornem inoperantes as instalações principais, as instalações de *backup* não são atingidas e tornam-se totalmente operacionais em condições idênticas em, no máximo, 48 (quarenta e oito) horas após decretado o estado de contingência.

5.1.9. Instalações técnicas de AR

As instalações técnicas de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICA MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [2].

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.1.1. A AC PRODEMGE BR segrega tarefas para funções críticas, com o intuito de evitar que qualquer empregado utilize indevidamente o sistema de certificação digital sem que seja detectado. As ações de cada empregado estão limitadas em função de seu perfil.

5.2.1.2. A AC PRODEMGE BR estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo-os em:

a) operações cotidianas do sistema;
b) gerenciamento e auditoria dessas operações;
c) gerenciamento de mudanças substanciais no sistema.

5.2.1.3. Todos os operadores da AC PRODEMGE BR recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal (Política de Segurança da AC), com base nas necessidades de cada perfil.

5.2.1.4. Quando um empregado se desliga das atribuições relativas à AC PRODEMGE BR, suas permissões de acesso são revogadas imediatamente. No caso de mudança na posição ou função do empregado dentro da própria AC, suas permissões de acesso são revistas. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado devolve à AC PRODEMGE BR no ato de seu desligamento das funções.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. O controle multiusuário, é necessário para a geração e a utilização da chave privada da AC PRODEMGE BR, 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 PRODEMGE BR necessitam da presença de no mínimo 2 (dois) de seus empregados com perfil qualificado. As demais tarefas da AC PRODEMGE BR podem ser executadas por um único empregado com perfil qualificado da AC PRODEMGE BR.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC PRODEMGE BR tem sua identidade e perfil verificados antes de:

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

5.2.3.2. Os certificados, contas e senhas utilizadas 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 PRODEMGE BR implementa um padrão de utilização de “senhas fortes”, definido da sua PS e em conformidade com o documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9], juntamente com os procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Todos os empregados da AC PRODEMGE BR que executam tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

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

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

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC PRODEMGE BR e AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é admitido conforme o estabelecido no documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9].

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 envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados da AC PRODEMGE BR e AR vinculadas, é submetido a:

a) verificação de antecedentes criminais;
b) verificação de situação de crédito;
c) verificação de histórico de empregos anteriores;
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 PRODEMGE BR e das AR vinculadas, envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da AC PRODEMGE BR e AR vinculadas;
b) sistema de certificação em uso na AC PRODEMGE BR;
c) procedimentos do Plano de Recuperação de Desastres (PRD);
d) procedimentos do Plano de Continuidade de Negócios;
e) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9 e 3.1.10 e;
f) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

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

5.3.5. Frequência e sequência de rodízio de cargos

A AC PRODEMGE BR não implementa o rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, suspeita ou real, realizada por pessoa encarregada de processo operacional da AC PRODEMGE BR ou das AR vinculadas, suspende, de imediato, o acesso do empregado ao seu sistema de certificação, instaura a abertura de Processo Administrativo para apuração dos fatos e, se for o caso, adota as medidas legais cabíveis.

5.3.6.2. O Processo Administrativo, indicado em 5.3.6.1 contém 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 PRODEMGE BR 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

O pessoal da AC PRODEMGE BR e das AR vinculadas, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é contratado conforme o estabelecido no documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9].

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC PRODEMGE BR disponibiliza para todo o seu pessoal, e para o pessoal das AR vinculadas:
a) sua DPC;
b) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [9];
c) documentação operacional relativa às suas atividades;
d) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a Política de Classificação de Informação (PCI) definida pela AC PRODEMGE BR e é mantida atualizada.

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 PRODEMGE BR é gerado pela própria AC PRODEMGE BR, em hardware específico, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

A geração do par de chaves de AC PRODEMGE BR é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC PRODEMGE BR, treinados para a função.

A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves da AC PRODEMGE BR é gerado em módulos criptográficos de hardware, no padrão obrigatório (com NSH3, Homologação da ICP-Brasil ou Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no DOC-ICP-01.01.

6.1.1.2. O par de chaves criptográficas de uma AC de nível imediatamente subsequente ao da AC PRODEMGE BR é gerado somente pelo titular do certificado correspondente. É gerado em módulo criptográfico homologado conforme o padrão ICP-Brasil NSH3.

6.1.1.3. Não se aplica.

6.1.2. Entrega da chave privada à entidade titular

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

6.1.3. Entrega da chave pública para emissor de certificado

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

6.1.3.2 A AC de nível imediatamente subsequente ao da AC PRODEMGE BR entrega à AC PRODEMGE BR cópia de sua chave pública, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8]. Essa entrega é feita por representante legalmente constituído da AC subsequente, em cerimônia específica, em data e hora previamente estabelecidas pela AC PRODEMGE BR. 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 PRODEMGE BR disponibiliza o seu certificado e todos os certificados da cadeia de certificação para os usuários da ICP-Brasil, através endereço *web*: http://icp-brasil.ac.prodemge.gov.br/repositorio.

6.1.5. Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho das chaves criptográficas associadas a certificados de AC subsequentes é de RSA 4096 (quatro mil e noventa e seis) bits para a cadeia de certificação V5, observando o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8].

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC PRODEMGE BR adotam no padrão obrigatório (com NSH3, 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 [8].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas referenciadas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8].

6.1.8. Geração de chave por hardware *ou* software

6.1.8.1. As chaves da AC PRODEMGE BR são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão obrigatório (com NSH3, 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 [8].

6.1.8.2. Não se aplica.

6.1.9. Propósitos de uso de chave (conforme o campo "*key usage"* na X.509 v3)

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

6.1.9.2. A chave privada da AC PRODEMGE BR é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

6.2. Proteção da Chave Privada

A chave privada da AC PRODEMGE BR é gerada, armazenada e utilizada apenas em hardware criptográfico com padrão de segurança de acordo com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8].

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC PRODEMGE BR adota o padrão "Homologação da ICP-Brasil NSH3 ou Certificação do INMETRO" definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8].

6.2.1.2. O padrão requerido para os módulos de geração de chaves criptográficas das AC de nível imediatamente subsequente ao da AC PRODEMGE BR está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8].

6.2.2. Controle "n de m" para chave privada

6.2.2.1. A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC PRODEMGE BR é dividida em "05" (cinco) partes e distribuídas por "05" (cinco) custodiantes designados pela AC PRODEMGE BR (m).

6.2.2.2. É exigido a presença de 2 (dois) custodiantes (n), formalmente designados pela AC PRODEMGE BR, para a ativação do componente e a consequente utilização da chave privada.

6.2.3. Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, 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 (backup) de chave privada

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

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

6.2.4.3. A AC PRODEMGE BR não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subsequente ao seu.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada cifrada por algoritmo AES-256 bits CBC, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8], e protegida com nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas das AC subordinadas à AC PRODEMGE BR não são arquivadas pela AC PRODEMGE BR.

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

6.2.6. Inserção de chave privada em módulo criptográfico

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

6.2.7. Método de ativação de chave privada

Para a ativação das chaves privadas exige-se um número mínimo de pessoas. A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Esse número mínimo é:

a) 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco) pessoas para utilização das suas chaves privadas criadas na cadeia V5.

Como a AC PRODEMGE BR não emite certificados para usuários finais, não há procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

6.2.8. Método de desativação de chave privada

A chave privada da AC PRODEMGE BR está instalada em ambiente físico com nível de segurança 4, onde só é permitido o acesso por pelo menos 2 funcionários autorizados. Sua desativação é feita por meio de comandos executados pelos funcionários de confiança, identificados e autorizados através de mecanismos nativos do sistema operacional.

Como a AC PRODEMGE BR não emite certificados para usuários finais, não há procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.9. Método de destruição de chave privada

Para a destruição das chaves privadas da AC PRODEMGE BR exige-se um número mínimo de pessoas. A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. Esse número mínimo é:

a) 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco) pessoas para utilização das suas chaves privadas criadas na cadeia V5.

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

Como a AC PRODEMGE BR não emite certificados para usuários finais, não há procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

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

6.3.2. Períodos de uso para as chaves pública e privada

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

6.3.2.2. Não se aplica.

6.3.2.3. Não se aplica.

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

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. A AC PRODEMGE BR garante que os dados de ativação da sua chave privada são únicos e aleatórios, instalados fisicamente em dispositivos criptográficos de controle de acesso.

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação

6.4.2.1. Os dados de ativação da chave privada da AC PRODEMGE BR são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Não se aplica.

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

6.5.1.2. Os requisitos gerais de segurança computacional dos equipamentos utilizados para a

geração dos pares de chaves criptográficas das AC subsequentes de certificados emitidos pela AC PRODEMGE BR, devem ser os mesmos descritos no item abaixo para os computadores servidores da AC PRODEMGE BR.

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

a) controle de acesso aos serviços e perfis da AC PRODEMGE BR;
b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC PRODEMGE BR;
c) uso de criptografia para segurança de base de dados;
d) geração e armazenamento de registros de auditoria da AC PRODEMGE BR;
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 com mecanismos de segurança física.

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

6.5.1.6. Qualquer equipamento incorporado à AC PRODEMGE BR é preparado e configurado como previsto na PS implementada, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A AC PRODEMGE BR aplica configurações de segurança definida como Evaluated Configuration Guide for Red Hat Enterprise Linux - EAL3, baseada na Common Criteria, que disponibiliza as atualizações deste sistema operacional utilizado nos servidores do Sistema de Certificação Digital.

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.

6.5.3.2. 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 PRODEMGE BR adota o Sistema de Gerencia de Certificados (SGC), desenvolvido em código aberto, integrantes do Projeto João de Barro (YWYRA/HAWA). Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e, após concluídos os testes, são colocados em um ambiente de homologação. Finalizando o processo de homologação das customizações, a gerência responsável avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. As ferramentas e os procedimentos empregados pela AC PRODEMGE BR garantem que os seus sistemas implementam os níveis configurados de segurança:

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

b) A AC PRODEMGE BR opera em equipamento off-line para geração, emissão de LCR e assinatura de certificados de AC subsequentes. Este ambiente não necessita de configuração de segurança de rede.

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

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

b) Implantação ou modificação de AC com customizações de certificados, páginas web, scripts, etc.;

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

d) Instalação de novos serviços na plataforma de processamento.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

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

6.7. Controles de Segurança de Rede

6.7.1. Diretrizes Gerais

O computador servidor da AC PRODEMGE BR que hospeda o sistema de certificação opera off-line, fisicamente desconectado de qualquer rede.

6.7.1.1. Não se aplica.

6.7.1.2. Não se aplica.

6.7.1.3. Não se aplica.

6.7.1.4. Não se aplica.

6.7.1.5. Não se aplica.

6.7.2. *Firewall*

6.7.2.1. Não se aplica.

6.7.2.2. Não se aplica.

6.7.3. Sistema de detecção de intrusão (IDS)

6.7.3.1. Não se aplica.

6.7.3.2. Não se aplica.

6.7.3.3. Não se aplica.

6.7.4. Registro de acessos não autorizados à rede
Não se aplica.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela AC PRODEMGE BR para o armazenamento de sua chave privada implementa as características de segurança do padrão “Homologação da ICP-Brasil NSH-3 ou Certificação do INMETRO”, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8]

O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada utilizada na geração de uma assinatura é única e seu sigilo é protegido por mecanismos de segurança internacionalmente aceitos;
b) a chave privada utilizada na geração de uma assinatura não pode ser deduzida, por mecanismos conhecidos, e é protegida contra decifração e falsificações, através de tecnologias e procedimentos de segurança internacionalmente aceitos;
c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Este meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

7. PERFIS DE CERTIFICADO E LCR

7.1. Diretrizes Gerais

7.1.1. Nos itens a seguir, desta DPC, estão descritos os aspectos dos certificados e LCR, emitidos pela AC PRODEMGE BR.

7.1.2. Não se aplica.

7.1.3. A AC PRODEMGE BR especifica, nos itens seguintes, o formato dos certificados emitidos para as AC subsequentes.

7.2. Perfil do Certificado

Todos os certificados emitidos pela AC PRODEMGE BR estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.2.1. Número (s) de versão

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

7.2.2. Extensões de certificado

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

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

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 cRL*Sign* estão ativados;

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

d.1) o campo policyIdentifier deve conter:

i. OID desta DPC: 2.16.76.1.1.125;

ii. não se aplica.

d.2) o campo policyQualifiers contém o endereço web da DPC AC PRODEMGE BR: http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge.pdf

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

f) "CRL Distribution Points", não crítica: contém o endereço Web onde se obtém a LCR da AC PRODEMGE BR:
http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_br/lcr_ac_prodemge.crl

7.2.3. Identificadores de algoritmo

Os certificados emitidos pela AC PRODEMGE BR são assinados com o uso do algoritmo RSA com SHA-512 na cadeia de certificação V5, conforme padrão PKCS#1 e de acordo com o documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [8].

7.2.4. Formatos de nome

Para os certificados emitidos pela AC PRODEMGE BR, o nome do titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISSO 9594, da seguinte forma:
C = BR
O = ICP-Brasil
OU = Nome de AC emitente
CN =Nome da AC titular

7.2.5. Restrições de nome

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

a) os acentos não devem ser utilizados e devem ser substituídos pelo caractere não acentuado;

b) o caractere "ç" deve ser substituído pelo caractere 'c';

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

Caractere	Código NBR9611 (Hexadecimal)	Caractere	Código NBR9611 (Hexadecimal)	Caractere	Código NBR9611 (Hexadecimal)
Branco	20	**(**	28	**:**	3ª
!	21	**)**	29	**;**	3B
"	22	*****	2ª	**=**	3D
#	23	**+**	2B	**?**	3F
$	24	**,**	2C	@	40
%	25	**-**	2D	****	5C
&	26	**.**	2E		
'	27	**/**	2F		

7.2.6. OID (*Object Identifier*) de DPC

O OID desta DPC é 2.16.76.1.1.125.

7.2.7. Uso da extensão "*Policy Constraints*"

Não se aplica.

7.2.8. Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "*Certificate Policies*" contém o endereço web da DPC AC PRODEMGE BR:
http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge.pdf

7.2.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.3. Perfil de LCR

7.3.1. Número (s) de versão

As LCR geradas pela AC PRODEMGE BR implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2. Extensões de LCR e de suas entradas

7.3.2.1. Neste item, são descritas todas as extensões de LCR utilizadas pela AC PRODEMGE BR e sua criticidade.

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

a) **"*Authority Key Identifier*", não crítica**: contém o *hash* da chave pública da AC PRODEMGE BR que assina a LCR;

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

8.ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta DPC será submetida à aprovação da AC Raiz. A DPC será alterada sempre que a legislação assim o exigir.

8.2. Políticas de publicação e notificação

A DPC da AC PRODEMGE BR está disponível no endereço web http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_br/dpc_ac_prodemge.pdf.
A AC PRODEMGE BR mantém essas informações sempre atualizadas.

8.3. Procedimentos de aprovação

Esta DPC foi submetida à aprovação, durante o processo de credenciamento da AC PRODEMGE BR, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7].

9. DOCUMENTOS REFERENCIADOS

9.1. 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 ICP-Brasil
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[2]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[4]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[5]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[9]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[10]	DIRETRIZES PARA SINCRONIZAÇÃO DE FREQUÊNCIA E DE TEMPO NA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL	DOC-ICP-07

9.2. Os documentos abaixo são aprovados por instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código ICP-Brasil
[8]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[3]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03

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

Ref.	Nome do documento	Código ICP-Brasil
[6]	TERMO DE TITULARIDADE – PESSOA JURÍDICA	ADE-ICP-05.B – PJ