Declaração de Práticas de Certificação da Autoridade Certificadora Prodemge

(DPC AC PRODEMGE SSL)

OID: 2.16.76.1.1.128

Classificação: Pública

Versão 2.1

Agosto de 2020

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
1.1	21/02/2019	Resolução 139	3.1.1.4.1, 3.1.1.11, 3.1.13, 4.4.2	Criação da Política de Certificado para Objetos Metrológicos – OM-BR no âmbito da ICP-Brasil.
		Resolução 136	3.1.10.1.3, 4.1.1.c	Aprovação dos procedimentos para criação do termo de titularidade
		Resolução 119	2.7.1	Obrigatoriedade de realização de auditorias WebTrust
1.2	22/05/2019	Adequações da AC PRODEMGE SSL	6.1.4	Acréscimo de endereço web de certificado
			1.3.5, 7.1.2	Inclusão da política de certificado tipo A3
1.3	28/06/2019	Resolução 151	Vários	Adequações à Resolução
2.0	09/06/2020	Resoluções 153, 154, 155, 156 e 164	1.1.1, 1.1.3, 1.1.5, 1.1.6, 1.2.2, 1.3.1, 1.3.2.1, 1.3.3, 1.3.5.1, 1.5.3, 1.6, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.2.1, 2.2.2, 3.1.1.2, 3.1.2.1, 3.2, 3.2.2.1.3, 3.2.2.1.4, 3.2.2.2, 3.2.2.3.1, 3.2.2.4, 3.2.3.1.2, 3.2.3.1.2, 3.2.3.1.5, 3.2.3.1.6, 3.2.3.2.1, 3.2.3.2.2, 3.2.3.2.3, 3.2.5, 3.2.7.1.3, 3.2.7.1.4, 3.2.7.1.5, 3.2.7.2.1, 3.2.8.1, 3.2.8.2, 3.2.8.3, 3.2.9.3.1, 3.2.9.4, 3.2.9.4.1, 3.2.9.6, 3.3.1.2, 3.3.1.3, 3.3.2.3, 3.3.2.4, 3.4, 4.1, 4.1.2, 4.1.2.1.2, 4.1.2.2, 4.1.2.4, 4.2.2.1, 4.4.1.2, 4.5, 4.5.1.1, 4.9.1.2, 4.9.1.3, 4.9.1.4.1, 4.9.1.4.2, 4.9.1.5, 4.9.2. 4.9.3.2, 4.9.3.3, 4.9.3.4, 4.9.7.5, 4.9.13, 4.10.1, 5.1.2.1.2, 5.1.2.2.2, 5.2.1.3.1, 5.5.1, 5.5.2,	Inclusão de procedimentos por Videoconferência. Acertos de tempos verbais e formatações. Adequações ao DOC-ICP-05 V5.5 Correções diversas por orientação do ITI

VERSÃO	DATA	RESOLUÇÃO QUE APROVOU A ALTERAÇÃO	ITEM ALTERADO	DESCRIÇÃO DA ALTERAÇÃO
			5.7.1.1, 5.7.2, 5.7.3.1, 5.7.3.2, 5.7.4, 6.1.4, 6.1.7.1, 6.2.4.3, 6.3.1, 6.3.2.2, 6.6.4, 7.1.2, 7.1.3, 7.1.4.1, 7.1.5.1, 7.1.5.2, 7.1.8, 8.4.3, 9.3.2, 9.3.3.2, 9.3.3.3, 9.3.3.4, 9.4.3, 9.4.8, 9.6.1.1, 9.6.1.3, 9.6.1.5, 9.6.1.6, 9.6.3.2, 9.6.4.2, 9.12.1, 9.12.2, 10.2	
2.1	28/08/2020	Mudança de estrutura organizacional na Prodemge	1.5.2; 1.5.3	Alteração de contatos e responsabilidades

SUMÁRIO

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento descreve as práticas e os procedimentos empregados pela Autoridade Certificadora PRODEMGE SSL (AC PRODEMGE SSL), integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, na execução dos seus serviços. A AC PRODEMGE SSL está certificada em nível imediatamente subsequente ao da AC PRODEMGE BR certificada pela AC Raiz da ICP-Brasil.

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 [5].

1.1.3. A AC PRODEMGE SSL é emissora de certificados SSL, e são observados e descritos os princípios e critérios WebTrust.

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

1.1.5. A AC PRODEMGE SSL mantém todas as informações da sua DPC sempre atualizadas.

1.2. Nome do documento e Identificação

1.2.1. Esta DPC é chamada "Declaração de Práticas de Certificação da Autoridade Certificadora PRODEMGE SSL", integrante da ICP-Brasil, e conhecida como "DPC AC PRODEMGE SSL". O Object Identifier (OID) desta DPC, atribuído pela AC Raiz, após conclusão de seu processo de credenciamento, é 2.16.76.1.1.128.

1.2.2. A AC PRODEMGE SSL emissora de certificados para usuários finais é exclusiva e separada de acordo com o propósito de uso de chaves de autenticação de servidor (SSL/TLS).

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

Esta DPC refere-se unicamente, à AC PRODEMGE SSL integrante da ICP-Brasil e encontra-se publicada nos seguintes endereços web:

- https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2.
- http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_ssl/
- http://icp-brasil2.acprodemge.com.br/repositorio/dpc/ac_prodemge_ssl/

1.3.2. Autoridades de Registro

1.3.2.1. As Autoridades de Registro (AR) vinculadas à AC PRODEMGE SSL, 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 no endereço web da AC PRODEMGE SSL https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2, conforme itens abaixo:

a) relação de todas as AR credenciadas;
b) relação de AR que tenham se descredenciado da cadeia da AC PRODEMGE SSL, com respectiva data do descredenciamento.

1.3.3. Titulares do Certificado

Podem ser titulares de certificados pessoas jurídicas de direito público ou privado, nacionais ou estrangeiras.

No caso de certificado emitido para equipamento, o titular será a pessoa jurídica solicitante do certificado.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

1.3.5.1. A AC PRODEMGE SSL publica em endereço web https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2 a relação de todos os seus Prestadores de Serviços de Suporte (PSS) e Prestadores de Serviços Biométricos (PSBios).

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

A AC PRODEMGE SSL implementa as seguintes Políticas de Certificado Digital:

Para Certificados de Assinatura Digital:

- Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE SSL, PC A1 da AC PRODEMGE SSL, OID 2.16.76.1.2.1.95.

Nas PC correspondentes estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC PRODEMGE SSL e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

1.4.2. Uso proibitivo do certificado

Quando cabível, as aplicações para as quais existam restrições ou proibições para o uso desses certificados estão listados nas PCs implementadas.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

AC PRODEMGE SSL

1.5.2. Contatos

Endereço:	Rua da Bahia, 2277 – Bairro de Lourdes – Belo Horizonte – MG – CEP: 30.160-012
Telefone:	(31) 3339-1213 / (31) 3339-1336
Faz:	Não se aplica
Página web	wwws.prodemge.gov.br
E-mail:	acprodemge@prodemge.gov.br
Empresa:	Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE

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

Nome:	Danielle Leite Santana Carrilho
Telefone:	(31) 3339-1213 / (31) 98462-0530
E-mail	acprodemge@prodemge.gov.br
Área:	Gerência de Controle de Níveis de Serviço

1.5.4. Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI. Os procedimentos de aprovação da DPC da AC PRODEMGE SSL são estabelecidos a critério do CG da ICP-Brasil.

1.6. Definições a Acrônimos

Sigla	Descrição
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AGR	Agente de Registro
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoa Jurídica
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoa Física
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITI	Instituto Nacional de Tecnologia da Informação
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil

Sigla	Descrição
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCI	Política de Classificação de Informação
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
PJ	Pessoa Jurídica
POP	Proof of Possession
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PRD	Plano de Recuperação de Desastres
PSC	Prestador de Serviço de Confiança
Prodemge	Companhia de Tecnologia da Informação do Estado de Minas Gerais
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
TSE	Tribunal Superior Eleitoral
UF	Unidade de Federação

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1. A AC PRODEMGE SSL mantém disponível repositório atendendo as seguintes obrigações:

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

As publicações da AC PRODEMGE SSL podem ser consultadas através do protocolo http. Somente a AC PRODEMGE SSL, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas no seu repositório.

2.1.2. O repositório da AC PRODEMGE SSL é acessível publicamente através dos endereços web informados no item 2.1.4 e está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do tempo do mês.

As publicações da AC PRODEMGE SSL podem ser consultadas através do protocolo http. Somente a AC PRODEMGE SSL, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas no seu repositório.

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

2.1.4. A AC PRODEMGE SSL disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR:

- http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_ssl/
- http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_ssl/

2.2. Publicação de informações dos certificados

2.2.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC PRODEMGE SSL, obedecendo as regras e os critérios estabelecidos nesta DPC.

- http://icp-brasil.ac.prodemge.gov.br/repositorio/
- http://icp-brasil2.acprodemge.com.br/repositorio/

A disponibilidade das informações publicadas nos dois endereços é de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC PRODEMGE SSL https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2:

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

2.3. Tempo ou Frequência de Publicação

2.3.1. De modo a assegurar a disponibilização sempre atualizada de seus conteúdos:

a) os certificados são publicados imediatamente após sua emissão;
b) a publicação da LCR se dá conforme o item 4.9.7 da PC correspondente;
c) as versões ou alterações desta DPC e da PC são atualizadas no web site da AC PRODEMGE SSL após aprovação da AC Raiz da ICP-Brasil; e
d) os endereços das AR vinculadas são atualizadas no web site da AC PRODEMGE SSL

2.4. Controle de Acesso aos Repositórios

2.4.1. Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC PRODEMGE SSL, às PC implementadas e aos endereços das AR vinculadas. São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC PRODEMGE SSL verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital.

As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem os diretos de propriedade intelectual de terceiros.

A AC reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1. Atribuição de Nomes

3.1.1. Tipos de nomes

3.1.1.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o “distinguished name” do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular.

3.1.1.2. Não se aplica.

3.1.2. Necessidade dos nomes serem significativos

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

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Esta DPC estabelece que identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado emitido pela AC PRODEMGE SSL. Números ou letras adicionais podem 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 SSL se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

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

3.2. Validação inicial de identidade

Neste item estão descritos em detalhes os requisitos e procedimentos utilizados pelas ARs vinculadas à AC PRODEMGE SSL para realização dos seguintes processos:

a) identificação do titular do certificado: identificação da pessoa jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7, observado o quanto segue:

i. para certificados de pessoa física: não se aplica.

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

Nota: nos casos de falecimento dos responsáveis legais por quaisquer empresas de um modo geral, desde que haja decisão judicial com nomeação de inventariante e termo de compromisso de inventariante assinado, e nomeação expressa deste como administrador será admitida a pessoa nomeada na qualidade de responsável legal do Certificado Digital para todos os fins legais e administrativos.

b) emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC PRODEMGE SSL. A extensão Subject Alternative Name é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

3.2.1. Método para comprovar a posse de chave privada

A AR verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. As RFC 4210 e 6712 são utilizadas como referência para essa finalidade.

No caso em que sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos são descritos nessas PCs, no item correspondente.

3.2.2. Autenticação da identificação da organização

3.2.2.1. Disposições Gerais

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

3.2.2.1.2. Em sendo o titular do certificado pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

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

a) apresentação do rol de documentos elencados no item 3.2.2.2;
b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
c) presença física do responsável pelo certificado; e
d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo responsável pelo certificado.

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

3.2.2.1.4. Fica dispensado o disposto no item 3.2.2.1.3, alíneas “b” e “c” caso o responsável pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

3.2.2.2. **Documentos para efeitos de identificação de uma organização**

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

a) Relativos a sua habilitação jurídica:
   i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;
   ii. se entidade privada:
      1) ato constitutivo, devidamente registrado no órgão competente; e
      2) documentos da eleição de seus administradores, quando aplicável;
b) Relativos a sua habilitação fiscal:
   i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
   ii. prova de inscrição no Cadastro Específico do INSS – CEI.

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

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

3.2.2.3. **Informações contidas no certificado emitido para uma organização**

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

a) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[1];
b) Cadastro Nacional de Pessoa Jurídica (CNPJ)[2];
c) nome completo do responsável pelo certificado, sem abreviações[3]; e
d) data de nascimento do responsável pelo certificado[4].

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

3.2.2.4. **Responsabilidade decorrente do uso do certificado de uma organização**

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

---

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

3.2.3. 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 de identificação legalmente aceitos e pelo processo biométrico da ICP-Brasil.

3.2.3.1. Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original oficial, podendo ser física ou digital, por meio de barramento ou aplicação oficial, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado:

a) Registro de Identidade ou Passaporte, se brasileiro; ou
b) Título de Eleitor, com foto; ou
c) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
d) Passaporte, se estrangeiro não domiciliado no Brasil;
e) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[11]; e
f) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[11].

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

3.2.3.1.1. Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a etapa de verificação de certificados da pessoa física.

As evidências desse processo farão parte do dossiê eletrônico do requerente.

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

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

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

a) por agente de registro distinto do que realizou a etapa de identificação;
b) na sede da AR ou AR própria da AC; e
c) antes do início da validade do certificado, sendo este revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

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

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.2. Informações contidas no certificado emitido para um indivíduo

3.2.3.2.1. Não se aplica.

3.2.3.2.2. Não se aplica.

3.2.3.2.3. Não se aplica.

3.2.4. Informações não verificadas do titular do certificado

Não se aplica.

3.2.5. Validação das autoridades

Não se aplica.

3.2.6. Critérios para interoperação

Não se aplica.

3.2.7. Autenticação da identidade de equipamento ou aplicação

3.2.7.1. Disposições Gerais

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

3.2.7.1.2. Não se aplica.

3.2.7.1.3. Se o titular for pessoa jurídica, é feita a confirmação da identidade da organização e da pessoa física, nos seguintes termos:

a) Apresentação do rol de documentos elencados no item 3.2.2.2;
b) Apresentação do rol de documentos elencados no item 3.2.3.1 do responsável pelo certificado;
c) Presença física do responsável pelo certificado e assinatura do termo de titularidade e responsabilidade de que trata o item 4.1.

3.2.7.1.4. Não se aplica.

3.2.7.1.5. Fica dispensada a observância do item 3.2.2.1.3 alíneas “b” e “c” para certificados cujo titular seja pessoa jurídica nos seguintes casos:

a) quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e responsável, e cujos dados biométricos deste último tenham sido devidamente coletados; ou
b) quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo A3 ou superior, cuja titularidade é da mesma pessoa física responsável legal da organização e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

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

3.2.7.2.1. Para certificados de equipamento ou aplicação que utilizem URL na identificação do titular, é verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele endereço. Nesse caso deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

3.2.7.2.2. Não se aplica.

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

3.2.7.3.1. É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nos documentos apresentados:

a) URL ou nome da aplicação[5];
b) nome completo do responsável pelo certificado, sem abreviações[6];
c) data de nascimento do responsável pelo certificado[7];
d) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[8];
e) Cadastro Nacional de Pessoa Jurídica (CNPJ)[9].

3.2.7.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade e responsabilidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.2.3.2.

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

3.2.7.4.1. Disposições Gerais

3.2.7.4.2. Não se aplica.

3.2.7.4.3. Não se aplica.

3.2.7.4.4. Não se aplica.

3.2.7.5. **Procedimentos para efeitos de identificação de um equipamento SAT**

3.2.7.5.1. Não se aplica.

3.2.7.6. **Informações contidas no certificado emitido para um equipamento SAT**

3.2.7.6.1. Não se aplica.

3.2.7.6.2. Não se aplica.

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

3.2.7.7.1. Disposições gerais

3.2.7.7.2. Não se aplica.

3.2.7.7.3. Não se aplica.

3.2.7.7.4. Não se aplica.

---

[5] No campo Subject, como parte do Common Name, que compõe o Distinguished Name
[6] No campo Subject Alternative Name, OID 2.16.76.1.3.2
[7] No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.4
[8] No campo Subject Alternative Name, OID 2.16.76.1.3.8
[9] No campo Subject Alternative Name, OID 2.16.76.1.3.3

3.2.7.8. Procedimentos para efeitos de identificação de um equipamento metrológico

3.2.7.8.1. Não se aplica.

3.2.7.9. Informações contidas no certificado emitido para um equipamento metrológico

3.2.7.9.1. Não se aplica.

3.2.7.9.2. Não se aplica.

3.2.8. Procedimentos complementares

3.2.8.1. A AC PRODEMGE SSL mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro, bem como os Requisitos de Linha de Base e as Diretrizes de EV para SSL.

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

3.2.8.3. É mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada e armazenadas no ponto de centralização da AC PRODEMGE SSL, situada na Rua da Bahia, 2277, Bairro Lourdes – CEP 30160-912 Belo Horizonte – Minas Gerais, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

3.2.8.3.1. Não se aplica.

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

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

3.2.9. Procedimentos específicos

3.2.9.1. Não se aplica.

3.2.9.2. Não se aplica.

3.2.9.3. Não se aplica.

3.2.9.3.1. Módulo Eletrônico da AR dos Órgãos Gestores de Pessoas

Não se aplica.

3.2.9.3.2. Não se aplica.

3.2.9.4. Não se aplica.

3.2.9.4.1. Não se aplica.

3.2.9.5. **Disposições para a Validação de Solicitação de Certificados do Tipo OM-BR:**

Não se aplica.

3.2.9.6. Não se aplica.

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. Identificação e autenticação para rotina de novas chaves antes da expiração

3.3.1.1. No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC PRODEMGE SSL para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

3.3.1.2. Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2, 3.2.3 ou 3.2.7;
b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;
c) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;
d) solicitação por meio eletrônico dada nas alíneas 'b' e 'c', acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação a ser editada pela AC-Raiz ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;
e) confirmado atendimento pleno do desafio e da assinatura do termo de titularidade, o aplicativo de AR poderá emitir o certificado e encaminhá-lo ao solicitante; e
f) todas as evidências do processo acima constarão no dossiê do certificado

3.3.1.2.1. Não se aplica.

3.3.1.3. Caso sejam requeridos procedimentos específicos para as PC implementadas, os mesmos são descritos nessas PC, no item correspondente.

3.3.2. Identificação e autenticação para novas chaves após a revogação ou expiração do certificado

3.3.2.1. Após a revogação ou expiração do certificado, os procedimentos utilizados para confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo descritos nas PC implementadas.

3.3.2.2. Não se aplica.

3.3.2.3. Não se aplica.

3.3.2.4. No caso de uma organização titular de certificado expirado, cujo responsável pelo certificado seja o mesmo ora solicitando novo certificado, que foi previamente identificado e cadastrado presencialmente, e cujos dados biométricos tenham sido devidamente coletados, a geração de novo par de chaves poderá ser realizada mediante confirmação do respectivo cadastro, da organização e do responsável pelo certificado, por meio de videoconferência, conforme regulamentação editada no DOC-ICP-05.05[15].

3.4. Identificação e Autenticação para solicitação de revogação

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

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

Solicitações de revogação de certificados são registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. Solicitação do certificado

Neste item são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC PRODEMGE SSL e pelas ARs a ela vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos compreendem todas as ações necessárias tanto do indivíduo solicitante quanto das AC e AR no processo de solicitação de certificado digital e contemplam:

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

Nota 1: o termo de titularidade para certificados de usuários finais com propósito de uso EV SSL segue o padrão adotado no documento EV SSL.

Nota 2: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados SSL, de equipamento e aplicação) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo é feita a verificação da assinatura contra o documento de identificação.

Nota 3: As solicitações de emissão de certificados podem ser realizadas de forma presencial ou através de Videoconferência conforme regulamentado no DOC-05.05 [15].

4.1.1. Quem pode submeter uma solicitação de certificado

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

4.1.1.1. Não se aplica.

4.1.1.2. Não se aplica.

4.1.1.3. Não se aplica.

4.1.1.4. Não se aplica.

4.1.2. Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas. Caso haja obrigações específicas para as PCs implementadas, as mesmas são descritas nessas PCs, no item correspondente.

4.1.2.1. Responsabilidades da AC

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

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

4.1.2.1.3. Não se aplica.

4.1.2.2. Obrigações da AC

As obrigações da AC PRODEMGE SSL são as abaixo relacionadas:

a) operar de acordo com a sua DPC e com as PCs que implementa;
b) gerar e gerenciar os seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AR a ela vinculadas e de usuários finais
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - On-line Certificate Status Protocol);
k) publicar em sua página web sua DPC e as PCs aprovadas que implementa;
l) publicar, em sua página web, as informações definidas no item 2.2.2 deste documento;
m) publicar, em página web, informações sobre o descredenciamento de AR;
n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que

implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR; e
y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados.

4.1.2.3. Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

4.1.2.4. Obrigações das ARs

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

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC PRODEMGE SSL utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICPBRASIL[1];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC PRODEMGE SSL e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL[1], bem como Princípios e Critérios WebTrust para AR[14];
f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2, 3.2.3 e 3.2.7; e
h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR[14].

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

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

4.2.2. Aprovação ou rejeição de pedidos de certificado

4.2.2.1. Não se aplica.

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

4.2.3. Tempo para processar a solicitação de certificado

A AC PRODEMGE SSL cumpre os procedimentos determinados na ICP-Brasil.

Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

4.3.1.1. A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento do Termo de Titularidade, e dos demais documentos exigidos de acordo com as especificidades de cada tipo de certificado. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido.

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

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

O Titular é notificado da emissão e do método para a retirada do certificado.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

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

a) concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;
b) garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.1.2. A aceitação de todo certificado emitido é declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, a declaração é feita pela pessoa física responsável por esses certificados.

4.4.1.3. Não se aplica.

4.4.2. Publicação do certificado pela AC

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

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

A notificação se dará de acordo com item 2.2 da DPC da AC Raiz.

4.5. Usabilidade do par de chaves e do certificado

O titular do certificado para usuário final emitido pela AC PRODEMGE SSL deve operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementam, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.1.1. A AC PRODEMGE SSL utiliza a sua chave privada e garante a proteção dessa chave conforme o previsto na sua própria DPC.

4.5.1.2. Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos pela AC PRODEMGE SSL constantes dos termos de titularidade de que trata o item 4.1 são os abaixo relacionados:

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 na PC correspondente;
d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e
e) informar à AC PRODEMGE SSL qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

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

4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.1. Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2. Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3. Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4. Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

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

Em acordo com item 3.3 desta DPC.

4.6.6. Publicação de uma renovação de um certificado pela AC

Não se aplica.

4.6.7. Notificação de emissão de certificado pela AC para outras entidades

Em acordo com item 4.3 desta DPC.

4.7. Nova chave de certificado (Re-key)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica.

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

Não se aplica.

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica.

4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica.

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

Não se aplica.

4.8. Modificação de certificado

4.8.1. Circunstâncias para modificação de certificado

Não se aplica.

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6. Publicação de uma modificação de certificado pela AC

Não se aplica.

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

Não se aplica.

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

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

4.9.1.2. O certificado será obrigatoriamente revogado:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;
b) Quando for necessária a alteração de qualquer informação constante no mesmo;
c) Não se aplica; ou
d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3. A AC PRODEMGE SSL define ainda que:

a) A AC PRODEMGE SSL revogará, no prazo definido no item 4.9.3.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
b) O CG da ICP-Brasil ou AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

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

4.9.1.4.1. A AC PRODEMGE SSL que emite certificados SSL suporta requisições OCSP em conformidade com a RFC 6960 e/ou RFC5019 e requisitos WebTrust. Para certificados SSL, a resposta OCSP deve ter validade mínima de um dia e máxima de uma semana, sendo que a próxima atualização deve estar disponível a cada quatro dias.

4.9.1.4.2. A AC PRODEMGE SSL que emite certificados SSL provê garantias que uma LCR possa ser baixada em não mais do que três segundos por uma linha de telefone analógica, sobre uma condição normal de rede.

4.9.1.5. A autenticidade da LCR/OCSP é também confirmada por meio das verificações da assinatura da AC PRODEMGE SSL e do período de validade da LCR/OCSP.

4.9.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) Por solicitação do titular do certificado;
b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
d) Pela AC PRODEMGE SSL;
e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
g) Não se aplica;
h) Não se aplica;
i) Não se aplica.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. Uma solicitação de revogação é necessária para que AR responsável inicie o processo de revogação. O solicitante da revogação habilitado pode solicitar facilmente e a qualquer tempo a revogação de certificado, evitando assim a utilização indevida do certificado.

Instruções para a solicitação de revogação do certificado são obtidas em página web disponibilizada pela AC PRODEMGE SSL ou pela AR Responsável.

A revogação é realizada através de Formulário on-line contendo o motivo da solicitação de revogação mediante o fornecimento de dados e da frase de identificação indicada na solicitação de emissão do Certificado.

Caso o Titular ou o Responsável - no caso de certificados de pessoas jurídicas ou aplicações - não recorde a frase de identificação ou quando a revogação é solicitada diretamente pelo Titular sem a participação do Responsável, o Formulário de revogação é impresso e assinado e entregue na AR Responsável.

4.9.3.2. Como diretrizes gerais:

a) O Solicitante da revogação de um certificado é identificado;
b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC PRODEMGE SSL;
c) As justificativas para a revogação de um certificado são documentadas; e
d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado e com a atualização do status do certificado na resposta OCSP à base de dados da AC PRODEMGE SSL, quando aplicável.

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

4.9.3.4. Não se aplica.

4.9.3.5. A AC PRODEMGE SSL 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 LCR correspondente.

4.9.3.6. Não se aplica.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 desta DPC. O prazo para aceitação do certificado pelo seu titular é de 7 (sete) dias, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

4.9.4.2. Não se aplica.

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

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

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7. Frequência de emissão de LCR

4.9.7.1. Neste item é definida a frequência para a emissão de LCR referente a certificados de usuários finais.

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

4.9.7.3. Não se aplica.

4.9.7.4. Não se aplica.

4.9.7.5. Para certificados EV SSL as frequências de emissão de LCR devem ser implementadas e descritas em suas PCs, no item correspondente, em conformidade com os requisitos Webtrust.

4.9.8. Latência máxima para a LCR

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

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

A AC PRODEMGE SSL suporta os processos de revogação de certificados de forma on-line quando aplicável por força de contratação específica.

4.9.10. Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11. Outras formas disponíveis para divulgação de revogação

Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. O titular de certificado deve notificar imediatamente, através de solicitação on-line de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.9.12.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente na AR responsável, assinando formulário de solicitação de revogação, observado o item 4.4.3 desta DPC.

Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

4.9.13. Circunstâncias para suspensão

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

4.9.14. Quem pode solicitar suspensão

A AC PRODEMGE SSL pode solicitar suspensão quando aprovado pelo Comitê Gestor.

4.9.15. Procedimento para solicitação de suspensão

Os procedimentos de solicitação de suspensão serão dados por norma específica das DPC e PCs associadas.

4.9.16. Limites no período de suspensão

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

4.10. Serviços de status de certificado

4.10.1. Características operacionais

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

4.10.2. Disponibilidade dos serviços

Ver item 4.9.

4.10.3. Funcionalidades operacionais

Ver item 4.9.

4.11. Encerramento de atividades

4.11.1. Observado o disposto no item sobre descredenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6], este item da DPC descreve os requisitos e os procedimentos que serão adotados nos casos de extinção ou encerramento dos serviços da AC PRODEMGE SSL, de uma AR, PSS ou PSBios a ela vinculados.

4.11.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC PRODEMGE SSL 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 SSL:

a) Revogará todos os certificados gerados pela AC PRODEMGE SSL nos prazos estipulados nas PC implementadas após a publicação e comunicará às partes afetadas através de mensagem eletrônica.
b) Extinguirá os serviços de emissão de certificados.
c) 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.
d) Destruirá a chave privada da AC PRODEMGE SSL extinta seguindo o procedimento descrito na DPC Item 6.2.9.
e) Transferirá os dados e gravações da AC PRODEMGE SSL para a Autoridade Certificadora sucessora, aprovada pela AC Raiz.
f) Transferirá as chaves públicas dos certificados emitidos pela AC PRODEMGE SSL 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 SSL. 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.
g) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC PRODEMGE SSL.
h) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

No caso de falência, extinção da AR ou encerramento das atividades como AR vinculada a AC PRODEMGE SSL a AR deverá seguir os seguintes requisitos e procedimentos:

a) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados.

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

a) Publicará, em sua página 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.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

A AC PRODEMGE SSL não executa práticas de custódia e recuperação de chaves.

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

A AC PRODEMGE SSL não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

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 SSL 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. As instalações para equipamentos de apoio, tais como máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro.

As instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada.

Existem sistemas de aterramento e de proteção contra descargas atmosféricas

Existe iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

5.1.2. Acesso físico

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

5.1.2.1. Níveis de acesso

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

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

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

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

5.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC PRODEMGE SSL. Qualquer atividade relativa ao ciclo de vida dos

certificados digitais é executada a partir desse nível. Pessoas não envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

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

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

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

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

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

5.1.2.1.11. Na AC PRODEMGE SSL, existem ambientes de quarto nível para abrigar e segregar:

a) equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores - (Data Center);
b) equipamentos de produção off-line e cofre de armazenamento.
c) Equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores)

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Data Center. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

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

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

5.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre da sala de cerimônia (Nível 5). Cada um desses depósitos dispõe de fechadura individual.

Os dados de ativação da chave privada da AC PRODEMGE SSL são armazenados nesses depósitos.

5.1.2.2. Sistemas físicos de detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por 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 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

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

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

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

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

5.1.2.3. Sistema de controle de acesso

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

5.1.2.4. Mecanismos de emergência

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

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

5.1.3. Energia e ar condicionado

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

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

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

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

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

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

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

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

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

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

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

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio

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

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

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

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

5.1.6. Armazenamento de mídia

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

5.1.7. Destruição de lixo

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

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

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

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

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.1.1. A AC PRODEMGE SSL 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 SSL 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. Os operadores do sistema de certificação da AC PRODEMGE SSL recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.3.1. A AC PRODEMGE SSL realiza um exame, para emissão de certificados em cadeia do tipo SSL, nos operadores do sistema de certificação da AC, de acordo com os requisitos de princípios e critérios WebTrust Baseline.

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

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 SSL, 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 SSL necessitam da presença de no mínimo 2 (dois) de seus empregados com perfil qualificado. As demais tarefas da AC PRODEMGE SSL podem ser executadas por um único empregado com perfil qualificado da AC PRODEMGE SSL.

5.2.3. Identificação e autenticação para cada perfil

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

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

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 SSL implementa um padrão de utilização de “senhas fortes”, definido da sua PS e em conformidade com o documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com os procedimentos de validação dessas senhas.

5.2.4. Funções que requerem separação de deveres

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

5.3. Controles de Pessoal

Todos os empregados da AC PRODEMGE SSL, das AR e PSS vinculados encarregados 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 SSL 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 [8].

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados da AC PRODEMGE SSL 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 SSL 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 SSL e AR vinculadas;
b) sistema de certificação em uso na AC PRODEMGE SSL;
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 dos itens 3.2.2, 3.2.3 e 3.2.7;
f) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC PRODEMGE SSL 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 SSL.

5.3.5. Frequência e sequência de rodízio de cargos

A AC PRODEMGE SSL 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 SSL 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 SSL 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 SSL 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 [8].

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC PRODEMGE SSL disponibiliza para todo o seu pessoal, e para o pessoal das AR vinculadas:

a) sua DPC;
b) a PC correspondente;
c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
d) documentação operacional relativa às suas atividades;
e) contratos, normas e políticas relevantes para suas atividades.

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

5.4. Procedimentos de Log de Auditoria

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC PRODEMGE SSL com o objetivo de manter um ambiente seguro.

5.4.1. Tipos de eventos registrados

5.4.1.1. A AC PRODEMGE SSL registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

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

5.4.1.1.1. A AC PRODEMGE SSL audita até seis por cento dos certificados emitidos.

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

a) registros de acessos físicos;
b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e perfis qualificados;
d) relatórios de discrepância e comprometimento; e
e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

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

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

5.4.1.5. A documentação relacionada aos serviços da AC PRODEMGE SSL é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.4.1.6. A AC PRODEMGE SSL registram eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) os agentes de registro que realizaram as operações;
b) data e hora das operações;
c) a associação entre os agentes que realizaram a validação e aprovação e o certificado gerado;
d) a assinatura digital do executante.

5.4.1.7. A AC PRODEMGE SSL a que esteja vinculada a AR define, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2. Frequência de auditoria de registros

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

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

5.4.3. Período de retenção para registros de auditoria

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

5.4.4. Proteção de registros de auditoria

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

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

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

5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria

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

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

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

5.4.7. Notificação de agentes causadores de eventos

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

5.4.8. Avaliações de vulnerabilidade

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

5.5. Arquivamento de Registros

Nos itens seguintes da DPC está descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC PRODEMGE SSL e pelas ARs a ela vinculadas.

5.5.1. Tipos de registros arquivados

Os tipos de registros arquivados são:

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 SSL; e
g) Informações de auditoria previstas no item 5.4.1.

5.5.2. Período de retenção para arquivo

Os períodos de retenção por tipo de registro arquivado são:

a) As LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
b) Os dossiês dos titulares são retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e
c) As demais informações, inclusive os arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

5.5.3. Proteção de arquivo

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

5.5.4. Procedimentos de cópia de arquivo

5.5.4.1. A AC PRODEMGE SSL estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC PRODEMGE SSL, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

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

5.5.5. Requisitos para datação de registros

Os servidores da AC PRODEMGE SSL são sincronizados com a hora fornecida pela AC RAIZ por meio de sua Fonte Confiável do Tempo – FCT conforme DOC-ICP 07 [13]. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos. No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

5.5.6. Sistema de coleta de dados de arquivo (interno e externo)

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

5.5.7. Procedimentos para obter e verificar informação de arquivo

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

5.6. Troca de chave

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

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

A comunicação de expiração, junto com as instruções para a solicitação de um novo certificado é realizada através de e-mail enviado ao titular do certificado.

5.6.2. Não se aplica.

5.7. Comprometimento e Recuperação de Desastre

Os requisitos relacionados aos procedimentos de notificação e recuperação de desastres estão descritos no PCN da AC PRODEMGE SSL, estabelecido conforme o documento POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], para garantir a continuidade de seus serviços críticos.

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

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

5.7.1.2. Os procedimentos previstos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs, contem as seguintes informações:

a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;
b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;
c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários;
d) Documentação dos processos e procedimentos acordados;
e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e
f) Teste e atualização dos planos.

5.7.2. Recursos computacionais, software, e/ou dados corrompidos

Conforme procedimentos descritos no PCN da AC PRODEMGE SSL.

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

5.7.3.1. Certificado de entidade é revogado

Conforme procedimentos descritos no PCN da AC PRODEMGE SSL.

5.7.3.2. Chave de entidade é comprometida

Conforme procedimentos descritos no PCN da AC PRODEMGE SSL.

5.7.4. Capacidade de continuidade de negócio após desastre

Conforme procedimentos descritos no PCN da AC PRODEMGE SSL.

5.8. Extinção da AC

Conforme CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICPBRASIL[6].

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPC define as medidas de segurança implantadas pela AC PRODEMGE SSL para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. São também definidos outros controles técnicos de segurança utilizados pela AC PRODEMGE SSL e pelas ARs vinculadas na execução de suas funções operacionais.

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas da AC PRODEMGE SSL é gerado pela própria AC PRODEMGE SSL, em hardware específico, conforme detalhado em 6.1.8, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

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

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

O par de chaves da AC PRODEMGE SSL é gerado em módulo criptográfico de hardware no padrão obrigatório (Homologação da ICP-Brasil NSH-3) conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

Somente os titulares dos certificados emitidos pela AC PRODEMGE SSL geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC PRODEMGE SSL.

6.1.1.3. Cada PC implementada pela AC PRODEMGE SSL define o meio utilizado para armazenamento da chave privativa, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.1.1.4. O processo de geração do par de chaves da AC PRODEMGE SSL é feito por hardware.

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

6.1.1.6. Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC PRODEMGE SSL são os indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Os procedimentos utilizados pela AC PRODEMGE SSL para a entrega de sua chave pública à AC de nível hierárquico superior encarregada da emissão de seu certificado é definido pela AC superior.

6.1.3.2. A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer. Os procedimentos específicos aplicáveis são detalhados em cada PC implementada.

6.1.4. Entrega de chave pública da AC às terceiras partes

A AC PRODEMGE SSL disponibiliza o seu certificado e todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através endereços web:

Para certificados emitidos na AC PRODEMGE SSL

- http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl.p7c
- http://icp-brasil2.acprodemge.com.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl.p7c

Para certificados emitidos na AC PRODEMGE SSL V2

- http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7c
- http://icp-brasil2.acprodemge.com.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7c

6.1.5. Tamanhos de chave

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

6.1.5.2. Não se aplica.

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

6.1.6.1. Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

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

6.1.7.1. Os certificados de assinatura emitidos pela AC PRODEMGE SSL têm ativados os bits digitalSignature e keyEncipherment.

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

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

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

A chave privada da AC PRODEMGE SSL 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 [9].

Os titulares de certificados emitidos pela AC PRODEMGE SSL, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado de suas chaves privadas.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC PRODEMGE SSL adota o padrão

"Homologação da ICP-Brasil NSH3" definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão de homologação ICP-Brasil ou Certificação do INMETRO.

Cada PC implementada descreve os padrões do módulo criptográfico a ser utilizado pela entidade titular de certificado.

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 SSL é dividida em "05" (cinco) partes e distribuídas por "05" (cinco) custodiantes designados pela AC PRODEMGE SSL (m).

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

6.2.3. Custódia (escrow) de chave privada

A AC PRODEMGE SSL não implementa tal prática.

6.2.4. Cópia de segurança 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 SSL 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 SSL não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC.

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 [9], 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. A AC PRODEMGE SSL não arquiva cópias de chaves privadas de titulares de certificados.

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

6.2.7. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

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.

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

6.2.9. Método de desativação de chave privada

A chave privada da AC PRODEMGE SSL 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.

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

6.2.10. Método de destruição de chave privada

Para a destruição das chaves privadas da AC PRODEMGE SSL 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.

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

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da AC PRODEMGE SSL e dos titulares de certificados de assinatura digital, bem como as LCRs emitidas e sistemas de OCSP são armazenadas e geridas pela AC PRODEMGE SSL, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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

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

6.3.2.2. Não se aplica.

6.3.2.3. Cada PC implementada pela AC PRODEMGE SSL define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.3.2.4. A validade admitida para certificados da AC PRODEMGE SSL 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

Nos itens seguintes desta PC são descritos os requisitos de segurança referentes aos dados de ativação.

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

6.4.1. Geração e instalação dos dados de ativação

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

6.4.2. Proteção dos dados de ativação

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

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

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A AC PRODEMGE SSL 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 dos titulares de certificados emitidos pela AC PRODEMGE SSL são descritos em cada PC implementada.

6.5.1.3. Os computadores servidores, utilizados pela AC PRODEMGE SSL, 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 SSL;

b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC PRODEMGE SSL;
c) uso de criptografia para segurança de base de dados;
d) geração e armazenamento de registros de auditoria da AC PRODEMGE SSL;
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 SSL, 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 SSL. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC PRODEMGE SSL 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 SSL 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. Neste item estão descritos os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR para os processos de validação e aprovação de certificados.

6.5.3.2. Os requisitos abaixo correspondem aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

a) controle de acesso lógico ao sistema operacional;
b) exigência de uso de senhas fortes;
c) diretivas de senha e de bloqueio de conta;
d) logs de auditoria do sistema operacional ativados, registrando:
    i. iniciação e desligamento do sistema;
    ii. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
    iii. mudanças na configuração da estação;
    iv. tentativas de acesso (login) e de saída do sistema (logoff);
    v. tentativas não autorizadas de acesso aos arquivos de sistema;
    vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.
e) antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;
f) firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse

ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;

g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
h) sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
i) utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
j) impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
k) utilização de data e hora de Fonte Confiável do Tempo (FCT);

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC PRODEMGE SSL utiliza o Processo de Software Prodemge fundamentado nos modelos de referências: Unified Process – UP e Melhoria do Processo de Software Brasileiro – MPS.BR. Contém as abordagens: tradicional e ágil e utiliza os padrões de engenharia de software aplicáveis ao contexto da Prodemge. É iterativo, incremental, adaptativo, configurável e com foco na qualidade de software, possibilitando o desenvolvimento e a manutenção de software em diferentes plataformas tecnológicas.

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

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC PRODEMGE SSL verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. A AC PRODEMGE SSL utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3. Controles 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 PRODEMGE SSL são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7. Controles de Segurança de Rede

6.7.1. Diretrizes Gerais

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

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

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

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

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

6.7.2. Firewall

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

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

6.7.3. Sistema de detecção de intrusão (IDS)

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

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

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

6.7.4. Registro de acessos não autorizados à rede

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

6.8. Carimbo de Tempo

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. Perfil do Certificado

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

7.1.1. Número de versão

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

7.1.2. Extensões de certificado

Não se aplica.

7.1.3. Identificadores de algoritmo

Não se aplica.

7.1.4. Formatos de nome

Não se aplica.

7.1.4.1. Não se aplica.

7.1.5. Restrições de nome

7.1.5.1. Não se aplica.

7.1.5.2. Não se aplica.

7.1.6. OID (Object Identifier) da DPC

O OID desta DPC é **2.16.76.1.1.128**.

7.1.7. Uso da extensão "Policy Constraints"

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Não se aplica.

7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC PRODEMGE SSL implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

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

7.2.2.2. As LCR da AC PRODEMGE SSL obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões de LCR:

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

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

A AC PRODEMGE SSL implementa a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP

Em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. Frequência e circunstâncias das avaliações

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

8.2. Identificação/Qualificação do avaliador

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

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

8.3. Relação do avaliador com a entidade avaliada

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

8.4. Tópicos cobertos pela avaliação

8.4.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPCs, PCs, PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os

princípios e critérios definidos pelo WebTrust.

8.4.2. A AC PRODEMGE SSL recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3. As entidades da ICP-Brasil diretamente vinculadas à AC PRODEMGE SSL (AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC PRODEMGE SSL é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

8.5. Ações tomadas como resultado de uma deficiência

A AC PRODEMGE SSL age de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

8.6. Comunicação dos resultados

A AC PRODEMGE SSL age de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

Variável conforme definição interna Comercial.

9.1.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

Não são cobradas tarifas de revogação e de acesso à informação de status.

9.1.4. Tarifas para outros serviços

Não são cobradas tarifas de acesso à informação de status do certificado e à LCR, bem como tarifas de revogação e de acesso aos certificados emitidos.

9.1.5. Política de reembolso

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

9.2. Responsabilidade Financeira

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

9.2.1. Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2. Outros ativos

Conforme regramento desta DPC.

9.2.3. Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3. Confidencialidade da informação do negócio

9.3.1. Escopo de informações confidenciais

9.3.1.1. Como princípio geral, todo documento, informação ou registro fornecido à AC ou às AR é sigiloso.

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

9.3.2. Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas pela AC PRODEMGE SSL e pelas ARs a ela vinculadas, compreendem:

a) os certificados e a LCR/OCSP emitidos pela AC PRODEMGE SSL;
b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
c) as PCs implementadas pela AC PRODEMGE SSL;
d) a DPC da AC PRODEMGE SSL;
e) versões públicas de PS;
f) a conclusão dos relatórios de auditoria; e
g) informações requisitadas por determinação judicial.

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

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

a) qualquer PC aplicável;
b) qualquer DPC;
c) versões públicas de Política de Segurança – PS; e
d) a conclusão dos relatórios da auditoria.

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

9.3.3. Responsabilidade em proteger a informação confidencial

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

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

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

9.3.3.4. Não se aplica.

9.4. Privacidade da informação pessoal

9.4.1. Plano de privacidade

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

9.4.2. Tratamento de informação como privadas

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

9.4.3. Informações não consideradas privadas

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

9.4.4. Responsabilidade para proteger a informação privadas

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

9.4.5. Aviso e consentimento para usar informações privadas

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

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

Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou
b) por meio de pedido escrito com firma reconhecida.

9.4.6. Divulgação em processo judicial ou administrativo

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

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

9.4.7. Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8. Informações a terceiros

Como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC PRODEMGE SSL é fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.5. Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

A AC PRODEMGE SSL declara e garante o quanto segue:

9.6.1.1. Autorização para certificado

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

9.6.1.2. Precisão da informação

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

9.6.1.3. Identificação do requerente

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

9.6.1.4. Consentimento dos titulares

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

9.6.1.5. Serviço

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

9.6.1.6. Revogação

A AC PRODEMGE SSL revogará certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e no documento Baseline Requirements EV SSL Guidelines.

9.6.1.7. Existência Legal

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

9.6.2. Declarações e Garantias da AR

Em acordo com item 4 desta DPC.

9.6.3. Declarações e garantias do titular

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

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

9.6.4. Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
b) verificar, a qualquer tempo, a validade do certificado.

9.6.4.2. O certificado da AC PRODEMGE SSL é considerado válido quando:

i. tiver sido emitido pela AC PRODEMGE BR;
ii. não constar como revogado pela AC PRODEMGE BR;
iii. não estiver expirado; e
iv. puder ser verificado com o uso do certificado válido da AC PRODEMGE BR.

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

9.6.5. Representações e garantias de outros participantes

Não se aplica.

9.7. Isenção de garantias

Não se aplica.

9.8. Limitações de responsabilidades

A AC PRODEMGE SSL não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

9.9. Indenizações

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

9.10. Prazo e Rescisão

9.10.1. Prazo

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

9.10.2. Término

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

9.10.3. Efeito da rescisão e sobrevivência

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

9.11. Avisos individuais e comunicações com os participantes

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

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC é submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC PRODEMGE SSL disponibiliza páginas específicas com a versão corrente desta DPC para consulta pública, nos endereços Web:

- https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2
- http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_ssl/dpc_ac_prodemge_ssl.pdf
- http://icp-brasil2.acprodemge.com.br/repositorio/dpc/ac_prodemge_ssl/dpc_ac_prodemge_ssl.pdf

9.12.3. Circunstâncias na qual o OID deve ser alterado

Não se aplica.

9.13. Solução de conflitos

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

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

9.14. Lei aplicável

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

9.15. Conformidade com a Lei aplicável

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

9.16. Disposições Diversas

9.16.1. Acordo completo

Esta DPC representa as obrigações e deveres aplicáveis à AC e AR. Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2. Cessão

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

9.16.3. Independência de disposições

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

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

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

10. DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICPBRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA	DOC-ICP-03

	ICP-BRASIL	
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[13]	DIRETRIZES PARA SINCRONIZAÇÃO DE FREQUÊNCIA E DE TEMPO NA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL	DOC-ICP-07

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

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL	DOC-ICP-01.01
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	DOC-ICP-05.02
[11]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03
[12]	REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS	DOC-ICP-01.02
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICA DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICPBRASIL	DOC-ICP-05

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

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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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