PRESIDÊNCIA DA REPÚBLICA
SECRETARIA-GERAL
SECRETARIA DE ADMINISTRAÇÃO
DIRETORIA DE TECNOLOGIA

Declaração de Práticas de Certificação
da
Autoridade Certificadora
da
Presidência da República

(DPC ACPR)

Infraestrutura de Chaves Públicas Brasileira

ICP-Brasil

ÍNDICE

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
AR - Autoridades de Registro
CEI - Cadastro Específico do INSS
CG - Comitê Gestor
CMM-SEI - Capability Maturity Model do Software Engineering Institute
CMVP - Cryptographic Module Validation Program
CN - Common Name
CNE - Carteira Nacional de Estrangeiro
CNPJ - Cadastro Nacional de Pessoas Jurídicas -
COBIT - Control Objectives for Information and related Technology
COSO - Comitee of Sponsoring Organizations
CPF - Cadastro de Pessoas Físicas
DMZ - Zona Desmilitarizada
DN - Distinguished Name
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira
IDS - Sistemas de Detecção de Intrusão
IEC - International Electrotechnical Commission
ISO – International Organization for Standardization
ITSEC - European Information Technology Security Evaluation Criteria
ITU - International Telecommunications Union
LCR - Lista de Certificados Revogados
NBR - Norma Brasileira
NIS - Número de Identificação Social
NIST - National Institute of Standards and Technology
OCSP - On-line Certificate Status Protocol
OID - Object Identifier
OU - Organization Unit
PASEP - Programa de Formação do Patrimônio do Servidor Público
PC - Políticas de Certificado
PCN - Plano de Continuidade de Negócio
PIS - Programa de Integração Social
POP - Proof of Possession
PSS - Prestadores de Serviço de Suporte
RFC – Request For Comments
RG - Registro Geral
SNMP - Simple Network Management Protocol
TCSEC - Trusted System Evaluation Criteria
TSDM - Trusted Software Development Methodology
UF - Unidade de Federação
URL - Uniform Resource Location

1. INTRODUÇÃO

1.1 Visão Geral

1.1.1. Esta Declaração de Práticas de Certificação - DPC ACPR descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da Presidência da República - ACPR no que se refere à emissão de certificados digitais S/MIME.

1.1.2. Esta DPC adota a estrutura recomendada pelo DOC-ICP-05 do Comitê Gestor da ICP-Brasil.

1.2 Identificação

Esta DPC possui o Identificador de Objeto (OID) 2.16.76.1.1.1, atribuído pela ICP-Brasil.

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridades Certificadoras

Esta DPC se refere unicamente à Autoridade Certificadora da Presidência da República – ACPR, integrante da ICP-Brasil.

1.3.2 Autoridades de Registro

1.3.2.1. O endereço da página web (URL) onde estão publicados os dados abaixo, referentes a Autoridade de Registro da ACPR responsável pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes é: https://certificados.serpro.gov.br/arpr.

a) relação de todas as AR credenciadas, com informações sobre as PC que implementam;
b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;
e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A ACPR mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1. A ACPR publica em sua página https://certificados.serpro.gov.br/arpr a relação de Prestadores de Serviço de Suporte - PSS;

1.3.3.2. PSS são entidades contratadas pela AC ou pela AR para desempenhar atividades que se classificam em uma das seguintes categorias:

a) disponibilizar infraestrutura física e lógica;
b) disponibilizar recursos humanos especializados; ou
c) disponibilizar infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A ACPR mantém as informações acima atualizadas.

1.3.4 Titulares de Certificado

1.3.4.1 Titulares de Certificados são as entidades, pessoas físicas ou jurídicas, autorizadas a receber um certificado digital emitido pela ACPR, segundo esta DPC.

1.3.4.2 Podem ser titulares de certificados emitidos pela ACPR as pessoas que atendam aos seguintes requisitos:

a) Servidores integrantes da estrutura da Presidência da República ou da Vice-Presidência da República que necessitam de certificados digitais para o exercício de suas funções;
b) Agentes públicos, indicados pelos Gestores dos Órgãos Essenciais da PR, que necessitam de certificados digitais para utilização em serviços geridos por esses órgãos. (Lista dos Órgãos

essenciais em: http://www2.planalto.gov.br/presidencia/estrutura-da-presidencia/estrutura-da-presidencia)

c) Autoridades que não pertencem ao Poder Executivo Federal, autorizadas pela Secretaria Geral a receberem certificados digitais.

1.3.5 Aplicabilidade

1.3.5.1 A ACPR implementa, sob esta DPC, a seguinte Política de Certificado:

- Política de Certificado do tipo A3 para Certificação de Pessoa Física ou Pessoa Jurídica, PC ACPR A3, OID 2.16.76.1.2.3.1.

1.3.5.2 As aplicações para as quais são adequados os certificados S/MIME emitidos pela ACPR e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para sua utilização, estão relacionadas na Política de Certificado correspondente.

1.4 Dados de Contato

A ACPR, responsável por esta DPC, funciona no seguinte endereço:

Diretoria de Tecnologia - DITEC
Anexo IV do Palácio do Planalto
Cep: 70.150-900
Brasília - DF

Pessoa de Contato

Nome:	Gustavo Adriane de Carvalho Freire
Telefones:	(61) 3411-2668 / 3411-2756 / 3411-1000
Fax:	(61) 3411-2855
E-mail:	acpr@presidencia.gov.br

2. DISPOSIÇÕES GERAIS

2.1 Obrigações e Direitos

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

2.1.1 Obrigações da ACPR

a) operar de acordo com esta DPC e com as respectivas PC 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 usuários finais;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCR;
k) publicar em página web a DPC e as PC aprovadas que implementa;
l) publicar em página web as informações definidas no item 2.6.1.2 deste documento;
m) publicar em página web as informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;
n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas nas DPC, PC e Política de Segurança – PS que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
v) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos; e
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações das AR

As obrigações da AR ACPR 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 à ACPR utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL[1];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;
f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela ACPR e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];
h) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil;
i) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
j) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10 e 3.1.11;
k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas.

2.1.3 Obrigações do Titular do Certificado

As obrigações dos titulares dos certificados, emitidos de acordo com esta DPC, são as constantes dos termos de titularidades de que trata o item 4.1.1 e incluem, no mínimo o seguinte:

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 nesta DPC, na PC correspondente e em outros documentos aplicáveis da ICP-Brasil;
e) informar à ACPR qualquer comprometimento de sua chave privada e providenciar a imediata revogação do certificado correspondente.

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

2.1.4 Direitos da Terceira Parte (Relying Party)

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

2.1.4.2. Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;
b) verificar, a qualquer tempo, a validade do certificado. Um certificado emitido pela ACPR é considerado válido quando:

c) não constar da LCR da ACPR;
d) não estiver expirado; e
e) puder ser verificado com o uso de certificado válido da ACPR.

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

2.1.5 Obrigações do Repositório

a) disponibilizar, logo após a sua emissão, a Lista de Certificados Revogados (LCR);
b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
c) implementar os recursos necessários para a garantia da segurança dos dados nele armazenados.

2.2 Responsabilidades

2.2.1 Responsabilidades da ACPR

2.2.1.1. A Autoridade Certificadora do ACPR responde pelos danos a que der causa.

2.2.1.2. A ACPR responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

2.2.1.3. Não se aplica.

2.2.1.4. Quando da emissão de certificado digital para servidores públicos da ativa e militares da União autorizados pelos responsáveis dos respectivos órgãos competentes, a responsabilidade por qualquer irregularidade na identificação do requerente do certificado incidirá sobre o órgão responsável pela identificação.

2.2.2 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

2.3 Responsabilidade Financeira

2.3.1 Indenizações devidas pela terceira parte usuária (Relying Party)

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

2.3.2 Relações Fiduciárias

Não existe situação específica de utilização do certificado da ACPR que requeira prática de indenização aos Usuários de Certificados. Surgindo qualquer solicitação será analisado caso a caso.

2.3.3 Processos Administrativos

Os processos administrativos cabíveis, relativos às operações da ACPR e de sua AR, seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

2.4 Interpretação e Execução

2.4.1 Legislação

2.4.1.1 Atos e regulamentos federais que regulam os assuntos do governo também regulam esta DPC, no que diz respeito a sua aplicação, construção, interpretação e validade. Isto inclui leis e regulamentos que governam os seguintes relacionamentos:

a) Governo Federal e seus funcionários, incluindo empregados contratados por tempo indeterminado ou temporários e consultores sobre contrato;
b) Governo Federal e organizações do setor privado com relações de negócio estabelecidas;
c) funcionários do Governo Federal com outros funcionários do Governo Federal;

2.4.1.2 Suportam ainda esta DPC a Medida Provisória 2200-2 de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil;

2.4.1.3 Esta DPC é também apoiada em uma estrutura contratual entre Presidência da República, Titulares de Certificados e qualquer Usuário de Certificado;

2.4.1.4 Os casos omissos deverão ser encaminhados para apreciação da AC Raiz.

2.4.2 Forma de interpretação e notificação

2.4.2.1. Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, a ACPR, examinará a disposição inválida e proporá, no prazo máximo de 30 dias, nova redação ou a retirada da disposição afetada.

2.4.2.2. As solicitações, notificações ou quaisquer outras comunicações relativas às práticas descritas nesta DPC serão realizadas por iniciativa da ACPR por intermédio de seus responsáveis e enviadas formalmente ao CG da ICP-Brasil.

2.4.3 Procedimentos de solução de disputa

2.4.3.1. Em caso de conflito entre esta DPC e outras declarações, documentos ou políticas da ACPR, esta DPC prevalecerá.

2.4.3.2. Esta DPC não prevalecerá sobre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nesta situação esta DPC será alterada para a solução da disputa.

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

2.5 Tarifas de Serviço

Nos itens a seguir, são especificadas as políticas tarifárias e de reembolso aplicáveis.

2.5.1 Tarifas de emissão e renovação de certificados

Não haverá incidência de tarifas para os órgãos pertencentes ao organograma da Presidência da República que não possuam previsão orçamentária na área de informática.

Para os demais órgãos poderá ser repassado o custo cobrado pela empresa prestadora de serviços de suporte para a ACPR.

2.5.2 Tarifas de acesso ao certificado

Não há tarifa que incida sobre este serviço.

2.5.3 Tarifas de revogação ou de acesso à informação de status

Não há tarifa que incida sobre este serviço

2.5.4 Tarifas para outros serviços

Não há tarifa que incida sobre este serviço.

2.5.5 Política de reembolso

Não há política de reembolso.

2.6 Publicação e Repositório

2.6.1 Publicação de informação da ACPR

2.6.1.1. A ACPR publica e mantém disponível em sua página web, no endereço https://certificados.serpro.gov.br/arpr, as informações descritas no item 2.6.1.2. A disponibilidade da página é de no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As informações publicadas na página da ACPR, são:

a) seu próprio certificado;
b) suas LCRs;
c) as DPC que implementa;
d) as PC que implementa;
e) a AR vinculada a ACPR e respectivo endereço de instalação técnica em funcionamento;
f) não se aplica;
g) uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2 Frequência de publicação

O certificado da ACPR e as LCRs são publicados imediatamente após sua emissão. As demais informações mencionadas no item 2.6.1 serão publicadas sempre que sofrerem alterações.

2.6.3 Controles de acesso

Não há nenhum controle de acesso de leitura das informações publicadas na página *web,* especificadas no item 2.6.1.

Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim.

Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

2.6.4 Repositórios

2.6.4.1. A ACPR adota como repositório de LCR os seguintes endereços:

- Para os certificados emitidos pela ACPR v1:

http://ccd.serpro.gov.br/lcr/ACPRv1.crl, http://ccd2.serpro.gov.br/lcr/ACPRv1.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv1.crl

- Para os certificados emitidos pela ACPR v2:

http://ccd.serpro.gov.br/lcr/ACPRv2.crl, http://ccd2.serpro.gov.br/lcr/ACPRv2.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv2.crl

- Para os certificados emitidos pela ACPR v3:

http://ccd.serpro.gov.br/lcr/ACPRv3.crl, http://ccd2.serpro.gov.br/ACPRv3.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv3.crl

- Para os certificados emitidos pela ACPR v4:

http://repositorio.serpro.gov.br/lcr/acprv4.crl, http://certificados2.serpro.gov.br/lcr/acprv4.crl e http://repositorio.icpbrasil.gov.br/lcr/acprv4.crl

2.6.4.2. A página https://certificados.serpro.gov.br/acpr, adotada como repositório de LCR atende aos seguintes requisitos:

a) disponibilidade – aquela definida no item 2.6.1;
b) protocolos de acesso – HTTP e HTTPS;
c) requisitos de segurança – obedece aos requisitos definidos no item 5.

2.7 Fiscalização e Auditoria de conformidade

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

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

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

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

2.7.5. A AR vinculada bem como seu Prestador de Serviço de Suporte receberam auditoria prévia, para fins de credenciamento. A ACPR é responsável pela realização de auditorias anuais de conformidade em todas as entidades a ela vinculadas, para fins de manutenção de credenciamento conforme documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

2.8 Sigilo

2.8.1 Disposições Gerais

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

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

2.8.1.3. A ACPR não emite certificados de sigilo.

2.8.2 Tipos de informações sigilosas

2.8.2.1. Todas as informações coletadas, geradas, transmitidas e mantidas pela ACPR e a AR vinculada são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3.

2.8.2.2. Como princípio geral, nenhum documento, informação ou registro fornecido a ACPR ou AR vinculada deverá ser divulgado.

2.8.3 Tipos de informações não sigilosas

Os seguintes documentos da ACPR e da AR vinculada são considerados documentos não sigilosos:

a) os certificados e as LCR emitidos;
b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
c) as PC implementadas;
d) esta DPC;
e) versões públicas de Políticas de Segurança;
f) a conclusão dos relatórios de auditoria.

2.8.4 Divulgação de informação de revogação/suspensão de certificado

2.8.4.1. A ACPR divulga informações de revogação de certificados por ela emitidos, no endereço web descrito no item 2.6.1.1 desta DPC, por meio de sua lista de certificados revogados.

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

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

2.8.5 Quebra de sigilo por motivos legais

A ACPR ou sua AR vinculada somente fornecerá documentos, informações ou registros sob sua guarda, mediante ordem judicial ou determinação legal.

2.8.6 Informações a terceiros

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

2.8.7 Divulgação por solicitação do titular

2.8.7.1. O titular do certificado ou seu representante legal tem acesso a quaisquer dos seus próprios dados e identificações e podem autorizar sua divulgação.

2.8.7.2. Qualquer liberação de informação do titular de certificado pela ACPR ou sua AR vinculada será permitida mediante autorização da seguinte forma:

a) por meio eletrônico, contendo assinatura digital do titular reconhecido pela ACPR;
b) por meio de documento formal, assinado pelo titular.

2.8.8 Outras circunstâncias de divulgação de informação

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

2.9 Direitos de Propriedade Intelectual

2.9.1. Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados e todos os documentos gerados para a ACPR (eletrônico ou não) pertencem e continuarão sendo propriedade da Presidência da República.

2.9.2. O Titular do Certificado concede a ACPR, o direito de publicar e divulgar em página Web, a chave pública que corresponde à chave privada que está em sua posse. Esta publicação ocorrerá pela incorporação da chave pública em certificado emitido pela ACPR.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Registro Inicial

3.1.1 Disposições Gerais

3.1.1.1. Neste item e nos seguintes a DPC descreve os requisitos e os procedimentos gerais utilizados pela AR, vinculada à ACPR, responsável para a realização dos seguintes processos:

a) Validação da solicitação de certificado: compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:

   I. confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado seja realmente àquela cujos dados constam na documentação apresentada, vedada qualquer espécie de procuração para tal fim;

   II. confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição. É admitida a procuração apenas se o ato constitutivo previr expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública, com poderes específicos para atuar perante a ICP-Brasil e com prazo de validade de até 90 (noventa) dias. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim;

   III. emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação para o segundo agente de registro efetuar a verificação da solicitação do certificado;

b) Verificação da solicitação de certificado: confirmação da validação realizada, executadas obrigatoriamente:

   I. Por agente de registro distinto do que executou a etapa de validação;

   II. Em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;

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

   IV. Antes do início da validade do certificado, sendo comandada a emissão do certificado no sistema de AC somente após a etapa da verificação ter ocorrido.

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

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

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

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

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

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

V. Para atender contratos firmados com entidades públicas cujos os editais de licitação tenham sido publicados até a data de publicação desta Resolução;

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

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

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

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

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

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

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

3.1.1.2.4. O local no qual a validação externa será realizada deverá ser informado no Formulário de Validação Externa, a que se refere a alínea “d” do item 3.1.1.2.5.

3.1.1.2.5. A validação fora do ambiente físico da AR deve atender ainda as seguintes condições:

a) utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR;

b) adotar aplicativo de georreferenciamento que permita rastrear o computador móvel utilizado na validação externa, sendo que a localização do equipamento deve ficar disponível no sistema da AR em que o agente de registro deva estar cadastrado previamente;

c) adotar equipamentos de coleta e verificação biométrica do titular e do agente de registro, em atendimento aos padrões da ICP-Brasil;

d) preencher o Formulário de Validação Externa, adendo ADE-ICP-05.D, o qual deverá ser assinado pelo agente de registro e pelo titular do certificado, preferencialmente assinados digitalmente;

e) em se tratando de dossiês físicos do titular de certificado, esses devem ser enviados para a Instalação Técnica em até 5 (cinco) dias úteis; e

f) Utilização de equipamento específico, destinado exclusivamente para fins de validação externa, vedada a utilização, para tal fim, das estações de trabalho ou outros equipamentos empregados na instalação técnica.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado são registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela ACPR, com a utilização de certificado digital ICP-Brasil S/MIME do tipo A3. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4. São mantidos arquivos com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias são mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

3.1.1.4.1. Não se aplica para a ACPR.

3.1.1.5. Não se aplica para a ACPR.

3.1.1.6. Não se aplica para a ACPR.

3.1.1.7. Cabe à ACPR disponibilizar para a sua Autoridade de Registro 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].

3.1.1.8. Não se aplica para a ACPR.

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

3.1.1.10. Não se aplica para a ACPR.

3.1.2 Tipos de nomes

3.1.2.1. Os tipos de nomes admitidos para os titulares de certificados da ACPR são:

a) certificados de pessoa física, o campo ”Common Name” (CN) é preenchido com o nome do Titular do Certificado;

b) certificados de pessoa jurídica, o campo “Common Name” (CN) é preenchido com o nome empresarial da pessoa jurídica;

3.1.2.2. A ACPR não emite certificados para AC subsequente.

3.1.3 Necessidade de nomes significativos

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

3.1.4 Regras para interpretação de vários tipos de nomes

Identificadores do tipo “*Distinguished Name*” (DN) devem ser únicos para cada titular de certificado, no âmbito da ACPR.

A AR pode propor e aprovar nomes distintos para candidatos de certificado.

3.1.5 Unicidade de nomes

“*Distinguished Name*” (DN) devem ser únicos e não ambíguos. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6 Procedimento para resolver disputa de nomes

A ACPR se reserva o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes de certificados. Durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.8 Método para comprovar a posse de chave privada

3.1.8.1. O sistema de certificação, implementado e utilizado pela ACPR controla e garante, de forma automática, a entrega do certificado somente ao detentor da chave privada correspondente à chave pública constante do certificado.

3.1.8.2. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem sua assinatura digital realizada com a chave privada correspondente à chave pública contida na solicitação. Ao recebê-la o software de certificação (SGC) verifica automaticamente a assinatura digital com uso da chave pública incluída nessa solicitação. Esse teste confirma a posse da chave privada pelo requisitante. A solicitação, com seu número de identificação, é então armazenada no banco de dados do SGC. Este número é impresso no Termo de Titularidade juntamente com os dados da entidade solicitante. Os dados são autenticados pela AR por meio da verificação das informações com base em originais de documentos oficiais, efetivando a vinculação da solicitação e chave privada à entidade autenticada pela AR.

3.1.8.3. A ACPR segue padrão RFC 2510, relativos a POP (*Proof of Possession*).

3.1.9 Autenticação da identidade de um indivíduo

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

3.1.9.1 Documentos para efeito de identificação de um indivíduo

Deverá ser apresentada documentação em versão original e, sempre que aplicável, coletada as biometrias, para fins de identificação de um indivíduo solicitante de certificado, conforme lista abaixo:

a) Cédula de Identidade ou Passaporte se brasileiro;
b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
c) Passaporte, se estrangeiro não domiciliado no Brasil;
d) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial;
e) Não se aplica para a ACPR;
f) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11];
g) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11];

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia. Caso os documentos tenham sido expedidos há mais de 5 (cinco) anos, ou não possuam fotografia, fornecer uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data de validação presencial.

NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador. O sistema de AC da ACPR disponibiliza para impressão a Declaração de Residência com base nas informações fornecidas pelo solicitante de certificado.

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

NOTA 4: Não se aplica.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a ACPR solicitará outro documento, preferencialmente a CNH – Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

NOTA 6: A ACPR poderá consultar as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

NOTA 7: Caso haja divergência dos dados constantes do documento de identidade, a ACPR suspenderá a emissão do certificado digital, orientando o solicitante a regularizar sua situação junto ao órgão responsável.

NOTA 8: Para a identificação de indivíduo na emissão de certificado digital para servidor público da ativa e militar da União, deverá ser observado o disposto item 3.1.1.9.

NOTA 9: É facultado aos Bancos Múltiplos e Caixa Econômica Federal autorizados a funcionar pelo BACEN, na identificação de titulares pessoa física de conta de depósito, utilizar o procedimento disposto no item 3.1.1.10.

3.1.9.2 Informações contidas no certificado emitido para um indivíduo

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

a) Nome completo, sem abreviações (*1);
b) Data de nascimento (*2);

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

c) Não se aplica para a ACPR.

3.1.9.2.2. A ACPR define também como obrigatório o preenchimento dos seguintes campos a partir da apresentação de um documento oficial que contenha essa informação:

a) Cadastro de Pessoa Física (CPF);
b) Número do Registro Geral – RG do titular e órgão expedidor;

NOTA: Os campos abaixo serão preenchidos caso o solicitante apresente o documento original de referência.

a) número de Identificação Social - NIS (PIS, PASEP ou CI);
b) número do Cadastro Especifico do INSS (CEI);
c) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;
d) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

3.1.9.2.3. A ACPR manterá arquivo com as cópias de todos os documentos utilizados.

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

NOTA 2: O cartão CPF poderá ser substituído por consulta à página da Receita Federal. Cópia dessa deverá ser arquivada junto à documentação, para fins de auditoria.

3.1.10 Autenticação da Identidade de uma organização

3.1.10.1 Disposições Gerais

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

3.1.10.1.2. Sendo titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado e detentora da chave privada. O responsável deverá ser, preferencialmente, o representante legal da pessoa jurídica ou um de seus representantes legais.

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

a) apresentação do rol de documentos elencados no item 3.1.10.2;
b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
c) presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do termo de titularidade de que trata o item 4.1.1;

3.1.10.2 Documentos para efeitos de identificação de uma organização

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

a) Relativos a sua habilitação jurídica:

   i. para pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo devidamente registrado no órgão competente e CNPJ;

ii. não se aplica. A ACPR não emite certificados para entidades privadas.

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.

3.1.10.3 Informações contidas no certificado emitido para uma organização

3.1.10.3.1. 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;
b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
c) nome completo e sem abreviações, CPF e data de nascimento do Representante Legal;
d) nome completo e sem abreviações, data de nascimento e CPF do responsável pelo certificado digital.

3.1.10.3.2 O preenchimento dos seguintes campos é opcional:

a) Cadastro Específico do INSS;
b) RG;
c) NIS – Identificador Social.

3.1.10.3.3. Cada PC pode definir como obrigatório o preenchimento de outros campos. Também 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 3.1.9.2.

3.1.11 Autenticação da Identidade de um equipamento ou aplicação

3.1.11.1. Disposições Gerais

Não se aplica.

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

Não se aplica

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

Não se aplica

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

Não se aplica

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

3.2.1. Antes da expiração do certificado de pessoa física, o titular de certificado pode solicitar um novo certificado na página Web https://certificados.serpro.gov.br/arpr da ACPR. Este será assinado digitalmente com o uso do certificado a ser renovado.

3.2.2. A renovação de certificados no âmbito da ACPR poderá ser efetuada pelo titular de certificado de acordo com uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;
b) solicitação de um novo pedido de certificado, conforme especificado no item 3.2.1, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva, permitida tal hipótese apenas para os certificados digitais de pessoa física.

3.2.3. Nos demais casos devem ser observados os mesmos requisitos e procedimentos exigidos para a solicitação inicial do certificado descritos na PC correspondente, item 4.1.

3.3 Geração de novo par de chaves após expiração ou revogação

3.3.1. O processo de identificação do solicitante quando da geração de novo par de chaves e emissão pela ACPR de novo certificado, após expiração ou revogação do anterior, será o mesmo da primeira emissão.

3.3.2. A ACPR não emite certificado para outra AC

3.4 Solicitação de Revogação

3.4.1. Os procedimentos para confirmação da identidade do solicitante de uma revogação são feitos conforme abaixo:

a) para as solicitações por meio de documento formal (oficio ou memorando) ou do Termo de Revogação disponibilizado na página de solicitação da ACPR, confrontação entre as assinaturas do documento de solicitação com as assinaturas constantes no Termo de Titularidade e nos documentos entregues quando da solicitação de certificação;
b) para as solicitações via e-mail assinado digitalmente, pela verificação da titularidade e validade do certificado;
c) para solicitação da AC Raiz ou do CG da ICP-Brasil, a confirmação será feita verificando-se a validade do documento (ofício ou memorando).

3.4.2. O documento apresentado para solicitação de revogação será arquivado junto ao dossiê do titular de certificado.

3.4.3 Quando a revogação for feita diretamente na pagina da ACPR, os dados e motivos da revogação serão registrados pelo sistema de AC, cujo acesso se dá por meio de assinatura digital.

4. REQUISITOS OPERACIONAIS

4.1 Solicitação de Certificado

4.1.1. Os requisitos e procedimentos mínimos necessários para as solicitações de emissão de certificado são:

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.1;
b) mediante o uso de certificado digital A3, a autenticação do AGR responsável pelas solicitações de emissão e de revogação de certificados; ou quando da emissão para servidores públicos da ativa e militares da União, por servidor público e militar autorizado pelos sistemas de gestão de pessoal dos órgãos competentes; e
c) um termo de titularidade assinado pelo titular do certificado e pelo responsável pelo uso do certificado, quando for certificado de pessoa jurídica, conforme adendo referente ao TERMO DE TITULARIDADE [4] específico, e, ainda, quando da emissão para servidor público da ativa e militar da União pela autoridade designada formalmente pelos órgãos competentes.

4.1.2. Não se aplica.

4.1.3. Não se aplica.

4.1.4. Não se aplica

4.2 Emissão de Certificado

4.2.1. Os certificados são emitidos pela ACPR de acordo com os seguintes passos:

a) o AGR verifica o completo e correto preenchimento da solicitação do certificado, bem como a documentação do solicitante;
b) o AGR aprova a solicitação, disponibilizando o certificado para a instalação por seu solicitante;
c) o software de AC emite automaticamente um e-mail informando ao solicitante que o certificado está disponível para instalação;

NOTA: O processo de validação da solicitação do certificado é realizado por Agente de Registro distinto do Agente que realiza a aprovação.

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

4.3 Aceitação de Certificado

4.3.1. Ao aceitar um certificado, seu titular está ciente que:

a) concorda com as responsabilidades, obrigações e deveres impostos a ele pelo Termo de Titularidade, pela PC A3 ACPR correspondente e por esta DPC;
b) garante que por seu conhecimento, nenhuma pessoa sem autorização terá acesso à chave privada associada ao certificado;

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

4.3.2. O recebimento de um certificado e seu uso subsequente constitui aceitação desse certificado por parte de seu titular

4.3.3 Não se aplica.

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 Circunstâncias para revogação

4.4.1.1. A ACPR pode revogar um certificado por ela emitido pelos seguintes motivos:

a) Exoneração ou suspensão do titular;
b) Mudança de cargo, função ou permissões do titular;
c) Falha do titular no cumprimento de suas obrigações ou qualquer compromisso, regulamento ou lei em vigor;
d) Solicitação de um dos responsáveis descritos no item 4.4.2;
e) Devolução da mídia armazenadora do certificado.

4.4.1.2. Um certificado é revogado obrigatoriamente pelos seguintes motivos:

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

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

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

4.4.2 Quem pode solicitar revogação

A solicitação para 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 ACPR;
e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz;
g) Não se aplica para a ACPR;
h) Não se aplica para a ACPR;
i) Por servidores públicos da ativa e militares da União autorizados pelos respectivos órgãos competentes pela identificação dos mesmos.

4.4.3 Procedimento para solicitação de revogação

4.4.3.1. Solicitações de revogação de certificados devem ser feitas da seguinte forma:

a) na página de solicitação, descrita no item 3.2.1, opção “Revogar Com Certificado”, onde o titular efetua a revogação, utilizando o próprio certificado a ser revogado;
b) na página de solicitação, “Revogar Com Senha”, onde o titular revoga seu certificado, informando o “Número de Referência”, o “Código de Acesso” e a “Senha” gerados na emissão do certificado;
c) com a entrega, na AR da ACPR, do Termo de Revogação disponibilizado na página de solicitação da ACPR, assinado pelo Titular de Certificado;
d) por meio de documento formal assinado pelo titular ou pelo responsável pelo órgão onde o titular exerce suas atividades profissionais;

e) por meio do formulário de Revogação de Certificado Digital, para usuários do Sistema SEI;
f) solicitação via e-mail assinado digitalmente;
g) por solicitação da AC Raiz ou do CG da ICP-Brasil;
h) pela devolução da mídia armazenadora do certificado.

4.4.3.2. Como diretrizes gerais, fica estabelecido que:

a) o solicitante da revogação de um certificado será identificado conforme item 3.4.1;
b) as solicitações de revogação, bem como as ações delas decorrentes são documentadas e registradas conforme descrito no item no item 3.4.2;
c) as justificativas para a revogação de um certificado são registradas por quem realizou a revogação no sistema de AC;
d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.4.3.3. 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 12 (doze) horas.

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

4.4.3.5. A ACPR responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a efetivação da revogação no sistema e a emissão da correspondente LCR.

4.4.3.6. Não se aplica.

4.4.4 Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1. Não há cobrança para solicitação de revogação de certificados no âmbito da ACPR.

4.4.4.2. Não se aplica.

4.4.5 Circunstâncias para suspensão

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

4.4.6 Quem pode solicitar suspensão

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

4.4.7 Procedimento para solicitação de suspensão

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

4.4.8 Limites no período de suspensão

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

4.4.9 Frequência de emissão de LCR

4.4.9.1. A LCR referente aos certificados emitidos pela ACPR é gerada, no máximo, a cada 6 (seis) horas.

4.4.9.2. Não se aplica.

4.4.9.3. Não se aplica.

4.4.9.4. Não se aplica**.**

4.4.10 Requisitos para verificação de LCR

4.4.10.1 Todo certificado deve ter a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado. Os certificados revogados da ACPR são listados nas LCR disponíveis nas páginas:

- http://ccd.serpro.gov.br/lcr/ACPRv1.crl, http://ccd2.serpro.gov.br/lcr/ACPRv1.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv1.crl
- http://ccd.serpro.gov.br/lcr/ACPRv2.crl , http://ccd2.serpro.gov.br/lcr/ACPRv2.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv2.crl

- http://ccd.serpro.gov.br/lcr/ACPRv3.crl, http://ccd2.serpro.gov.br/ACPRv3.crl e http://repositório.icpbrasil.gov.br/lcr/ACPRv3.crl
- http://repositorio.serpro.gov.br/lcr/acprv4.crl, http://certificados2.serpro.gov.br/acprv4.crl e http://repositório.icpbrasil.gov.br/lcr/acprv4.crl

4.4.10.2 A autenticidade da LCR/OCSP deve ser confirmada por meio da verificação da assinatura da ACPR e do período de validade da LCR/OCSP.

4.4.11 Disponibilidade para revogação/verificação de status on-line

A ACPR não suporta o processo de verificação da situação de estado de certificados de forma *on-line (OCSP)*. O processo de revogação on-line está disponível ao Titular do Certificado, conforme descrito no item 3.4.

4.4.12 Requisitos para verificação de revogação on-line

A ACPR não suporta o processo de verificação da situação de estado de certificados de forma on-line.

4.4.13 Outras formas disponíveis para divulgação de revogação

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

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

Item não aplicável.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deve notificar imediatamente a ACPR e solicitar a revogação de seu certificado conforme descrito no item 4.4.3.

4.4.15.2. Quando houver comprometimento ou suspeita de comprometimento da chave privada, o Titular do Certificado deverá comunicar imediatamente a ACPR.

4.5 Procedimentos de Auditoria de Segurança

4.5.1 Tipos de Evento Registrados

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

a) Iniciação e desligamento do sistema de certificação;
b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACPR;
c) Mudanças na configuração da ACPR ou nas suas chaves;
d) Mudanças nas políticas de criação de certificados;
e) Tentativas de acesso (*login*) e de saída do sistema (*logoff*);
f) Tentativas não autorizadas de acesso aos arquivos de sistema;
g) Geração de chaves próprias da ACPR ou de chaves de Titulares de Certificados;
h) Emissão e revogação de certificados;
i) Geração de LCR;
j) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
k) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável;
l) Operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A ACPR registra, eletrônica ou manualmente as seguintes informações de segurança não geradas diretamente pelo seu sistema de certificação:

a) Registros de acessos físicos;
b) Manutenção e mudanças na configuração de seus sistemas;
c) Mudanças de pessoal e de perfis qualificados;
d) Relatórios de discrepância e comprometimento; e

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

4.5.1.3. Os registros de auditoria mínimos a serem mantidos pela ACPR incluem além dos acima:

a) Registros de solicitação, inclusive registros relativos a solicitações rejeitadas;
b) Pedidos de geração de certificado, mesmo que a geração não tenha êxito;
c) Registros de solicitação de emissão de LCR.

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

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

4.5.1.6. A AR vinculada a ACPR registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos, obrigatórios, estão incluídos em arquivos de auditoria:

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

4.5.1.7. A ACPR define para cada AR vinculada, em documento a ser disponibilizado nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados, e dos termos de titularidade.

4.5.2 Frequência de auditoria de registros (logs)

A periodicidade de auditoria de registros não será superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da ACPR. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros para verificar se não foram alterados. Em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3 Período de Retenção para registros (logs) de Auditoria

A ACPR mantém localmente, nas instalações do Prestador de Serviço de Suporte, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4 Proteção de registro (log) de Auditoria

4.5.4.1. Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.4.2. As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.4.3. Os mecanismos de proteção descritos neste item obedecem a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

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

A ACPR executa procedimentos de backup, de todo o sistema de certificação (Sistema Operacional, Sistema de Aplicação e Banco de Dados) de duas formas:

a) Diariamente: cópia de segurança;

b) Semanalmente: cópia armazenada para processos de auditoria.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da ACPR é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de ACPR, pelo

sistema de controle de acesso e pelo pessoal operacional. A localização dos recursos se encontra na tabela abaixo:

Tipo de evento	SISTEMA DE COLEÇÃO	Registrado por
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de *log-in* e *log-out*	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados	Automático	AC ou Software de AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado	Automático	Software de AR
Logs de *Backup* e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de *software* e *hardware*	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	*Software* de controle de acesso e pessoal de operações

4.5.7 Notificação de agentes causadores de eventos

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

4.5.8 Avaliações de vulnerabilidade

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

4.6 Arquivamento de Registros

4.6.1 Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela ACPR:

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 ACPR;
g) informações de auditoria previstas no item 4.5.1.

4.6.2 Período de retenção para arquivo

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

a) as LCR referentes a certificados de assinatura digital são retidas permanentemente para fins de consulta histórica;
b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados e o termos de titularidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data da expiração ou revogação do certificado;

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

4.6.3 Proteção de arquivos

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

4.6.4 Procedimentos para cópia de segurança (backup) de arquivos

4.6.4.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da ACPR, e recebe o mesmo tipo de proteção utilizada no arquivo principal.

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

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

4.6.5 Requisitos para datação de registros

4.6.5.1. Os servidores de dados utilizados pela ACPR são sincronizados com a hora GMT fornecida pelo Observatório Nacional. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.

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

4.6.6 Sistema de coleta de dados de arquivo

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

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

4.6.7 Procedimentos para obter e verificar informação de arquivo

As informações de arquivos podem ser acessadas da seguinte forma:

a) Por pessoas autorizadas e corretamente identificadas, mediante apresentação de um instrumento devidamente constituído;
b) Por titulares de certificados ou seus representantes legais, mediante solicitação formal, conforme definido no item 2.8.6;
c) A própria AC por meio de seus funcionários ou os Agentes de Registros das AR vinculadas.

4.7 Troca de chave

4.7.1. A ACPR comunica ao Titular de Certificado, por e-mail, ao endereço cadastrado na solicitação do certificado, a necessidade de renovação do certificado, com antecedência mínima de 30 dias.

4.7.2. Não se aplica.

4.8 Comprometimento e Recuperação de Desastre

Nos itens a seguir estão relacionados procedimentos de notificação e de recuperação de desastres previstos no PCN da ACPR, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.8.1 Recursos computacionais, software e dados corrompidos

A ACPR possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que recursos computacionais, *software* e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

a) É feita a identificação de todos os elementos corrompidos;
b) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
c) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um *backup* de segurança até a revogação do certificado da ACPR.

4.8.2 Certificado de entidade é revogado

A ACPR possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que seu certificado tenha que ser revogado. Tais procedimentos podem ser resumidos no seguinte:

a) A AC Raiz é informada por comunicações seguras e são também notificados os titulares de certificado;
b) A ACPR revoga os certificados por ela emitidos;
c) A ACPR pede um novo certificado à AC Raiz;
d) Iniciam-se os procedimentos para emissão dos novos certificados de usuários.

Nota: Os usuários são instruídos a solicitar um novo certificado que será validado e aprovados de acordo com esta DPC.

4.8.3 Chave de entidade é comprometida

A ACPR possui um Plano de Continuidade de Negócio no qual está especificado que em caso de comprometimento da chave da ACPR, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas para ativar o *site* de contingência.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

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

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

4.8.5 Atividades das Autoridades de Registro

No PCN das AR vinculadas são previstos os seguintes procedimentos para recuperação total ou parcial das atividades das AR:

a) identificação dos eventos que causaram interrupções nos processos do negócio;
b) identificação das responsabilidades e procedimentos de emergência;
c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial é dada à recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;
d) documentação dos processos e procedimentos adotados;
e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
f) teste e atualização dos planos.

4.9 Extinção dos serviços da AC, AR ou PSS

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

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

a) Notificação para o e-mail do titular do certificado;
b) Transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta;
c) Preservação de quaisquer registros não transferidos a um sucessor;
d) As chaves públicas dos certificados emitidos pela AC dissolvida serão armazenadas por outra AC após aprovação da AC Raiz;
e) Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela ACPR;
f) A ACPR, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas;
g) Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

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

5.1 Controle Físico

5.1.1 Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação utilizado para a operação da ACPR não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Todos os aspectos de construção das instalações da ACPR, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos abaixo:

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

5.1.2 Acesso físico nas instalações de AC

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

5.1.2.1 Níveis de Acesso

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

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

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da ACPR, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. **O segundo nível – ou nível 2** – é interno ao primeiro nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da ACPR.

A passagem do primeiro para o segundo nível exige identificação por meio eletrônico, e o uso de crachá.

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

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

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

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

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

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

5.1.2.1.11. São três os ambientes de quarto nível abrigados pela sala cofre:

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

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

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

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

b) Possuir tranca com chave.

5.1.2.1.14. O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da ACPR estão armazenados em um desses depósitos.

5.1.2.2 Sistema físico de detecção

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

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, 1 (um) ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes.

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

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

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

5.1.2.3 Sistema de Controle de Acesso

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

5.1.2.4 Mecanismos de emergência

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

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

5.1.3 Energia e ar condicionado nas instalações da AC

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

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

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

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

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

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

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

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

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

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

a) Geradores de porte compatível;
b) Geradores de reserva;
c) Sistemas de *no-breaks* redundantes;
d) Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água nas instalações da AC

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

5.1.5 Prevenção e proteção contra incêndio nas instalações da AC

5.1.5.1. Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobre-aquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

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

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

5.1.6 Armazenamento de mídia nas instalações da AC

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

5.1.7 Destruição de lixo nas instalações da AC

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

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

5.1.8 Instalações de segurança (backup) externas (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.

5.1.9 Instalações técnicas de AR

As instalações técnicas de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

5.2 Controles Procedimentais

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

5.2.1 Perfis qualificados

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

5.2.1.2. A ACPR estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

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

5.2.1.4. Quando um empregado se desliga da AC, suas permissões de acesso são revogadas imediatamente.

5.2.1.5. Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da ACPR, conforme o descrito em 6.2.2.

5.2.2.3. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da ACPR necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da ACPR. As demais tarefas da ACPR podem ser executadas por um único operador.

5.2.3 Identificação e autenticação para cada perfil

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

a) Ser incluído em uma lista de acesso às instalações da ACPR;
b) Ser incluído em uma lista para acesso físico ao sistema de certificação da ACPR;
c) Receber um certificado para executar suas atividades operacionais na ACPR; e
d) Receber uma conta no sistema de certificação da ACPR.

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

a) São diretamente atribuídos a um único operador (funcionário da ACPR devidamente qualificado);
b) Não são compartilhados;
c) São restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A ACPR implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3 Controles de Pessoal

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

a) Os termos e as condições do perfil que ocupam;
b) O compromisso de observar as normas, políticas e regras aplicáveis da ACPR;
c) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e
d) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

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

5.3.2 Procedimentos de Verificação de Antecedentes

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

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

5.3.2.2. A ACPR poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal da ACPR e das ARs vinculadas, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados

recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e mecanismos de segurança da ACPR e das AR vinculadas;
b) Sistema de certificação em uso na ACPR;
c) Procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9, 3.1.10 e 3.1.11;
e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

Todo o pessoal da ACPR e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da ACPR. Treinamentos de reciclagem são realizados pela ACPR sempre que necessário.

5.3.5 Frequência e sequência de rodízios de cargos

A ACPR não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

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

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

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

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

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

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

5.3.7 Requisitos para contratação de pessoal

O pessoal da ACPR 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 na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.8 Documentação fornecida ao pessoal

5.3.8.1. A ACPR disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas, no mínimo:

a) Esta DPC;
b) A Política de segurança da ICP-Brasil;
c) A Política de Segurança da ACPR;
d) Documentação operacional relativa às suas atividades;
e) Contratos, normas e políticas relevantes para suas atividades.

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

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1 Geração e Instalação do Par de chaves

6.1.1 Geração do Par de Chaves

6.1.1.1. O par de chaves da ACPR é gerado pela própria ACPR, em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORÍTMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.1.1. O módulo criptográfico da ACPR v3 e ACPR v4 segue o padrão "Homologação da ICP-Brasil NSH-3";

6.1.1.1.2. O módulo criptográfico da ACPR v1 e ACPR v2 segue o padrão "FIPS (*Federal Information Processing Standards)* 140-2 *level 3".*

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

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

6.1.2 Entrega da chave privada à entidade titular

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

6.1.3 Entrega da chave pública para emissor de certificado

6.1.3.1. Não se aplica.

6.1.3.2. As chaves públicas dos solicitantes de certificados são entregues por meio de uma troca on-line utilizando funções automáticas do software de certificação da ACPR.

6.1.4 Disponibilização de chave pública da ACPR para usuários

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

a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].
b) Página https://certificados.serpro.gov.br/acpr;
c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1. Os tamanhos das chaves criptográficas associadas aos certificados emitidos pela ACPR estão definidos no mesmo item da Política de Certificados – PCA3 da ACPR.

6.1.5.2. Não se aplica.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos Titulares de certificado adotam, no mínimo, o padrão FIPS 140-1 ou equivalente estabelecido pelo CG da ICP-Brasil.

6.1.7 Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave é feita de acordo com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8 Geração de chave por *hardware ou software*

6.1.8.1. O processo de geração do par de chaves do Titular do Certificado é feito por hardware criptográfico e implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8.2. A PC A3, implementada pela ACPR, define o processo utilizado para a geração de chaves criptográficas dos titulares de certificados, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

6.1.9.1. Os certificados de assinatura emitidos pela ACPR têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela ACPR, bem como as possíveis restrições cabíveis em conformidade com as aplicações definidas para os certificados correspondentes, estão especificados em cada PC que implementa.

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

6.2 Proteção da Chave Privada

A chave privada da ACPR é gerada, armazenada e utilizada apenas em hardware criptográfico com padrão de segurança "Homologação da ICP-Brasil NSH-3", definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], não havendo, portanto, tráfego da mesma em nenhum momento.

6.2.1 Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da ACPR adota o padrão Homologação da ICP-Brasil NSH-3, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Os módulos de geração de chaves criptográficas dos Titulares de Certificados são aqueles definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] - Cada PC implementada especifica os requisitos adicionais aplicáveis.

6.2.2 Controle "n de m' para chave privada

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

6.2.2.2. É exigido a presença no mínimo de 2 (dois) detentores da chave de ativação ("n") de um grupo de 9 (nove ("m")) para a ativação da chave da ACPR.

6.2.3 Recuperação (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, Isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4 Cópia de segurança (backup) de chave privada

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

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

6.2.4.3. A ACPR não mantém cópia de segurança das chaves privadas de titulares de certificados de assinatura digital por ela emitido.

6.2.4.4. Não aplicável

6.2.5 Arquivamento de chave privada

6.2.5.1. As chaves privadas dos titulares de certificados emitidos pela ACPR não são arquivadas.

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

6.2.6 Inserção de chave privada em módulo criptográfico

A chave privada da ACPR é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7 Método de ativação de chave privada

A ativação da chave privada da ACPR é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de "2" de "9" dos *custodiantes* da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da ACPR. As senhas utilizadas obedecem à política de senhas estabelecida pelo Prestador de Serviço de Suporte da ACPR.

6.2.8 Método de desativação de chave privada

A chave privada da ACPR, armazenada em módulo criptográfico, é desativada quando não mais é necessária, através de mecanismo disponibilizado pelo software de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de "2" de "9" dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da Prestadora de Serviço de Suporte da ACPR. As senhas utilizadas obedecem à política de senhas por eles estabelecida.

6.2.9 Método de destruição de chave privada

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

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

As chaves públicas dos certificados da ACPR e dos titulares de certificados bem como as LCRs emitidas serão armazenadas, permanentemente, para verificação de assinaturas geradas durante o período de validade desses certificados.

6.3.2 Períodos de uso para as chaves pública e privada

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

6.3.2.2. Não se aplica.

6.3.2.3. As PC implementadas pela ACPR definem o período máximo de validade de seus certificados com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.4. O período máximo de validade admitido para o certificado da ACPR é de 10 (dez) anos.

6.4 Dados de ativação

Nos itens seguintes, estão descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Os requisitos específicos, quando existirem, serão descritos nas PC correspondentes.

6.4.1 Geração e instalação dos dados de ativação

6.4.1.1. A ACPR garante que os dados de ativação da sua chave privada são únicos e aleatórios.

6.4.1.2. Não se aplica.

6.4.2 Proteção dos dados de ativação

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

6.4.2.2. Não se aplica.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança dos computadores

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1. A ACPR 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 do equipamento onde são gerados os pares de chaves criptográficos dos titulares de certificados emitidos pela ACPR estão descritos no item 6.5.1 da PC implementada.

6.5.1.3. Os computadores servidores, utilizados pela ACPR, 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 ACPR;
b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da ACPR;
c) Acesso restrito aos bancos de dados da ACPR;
d) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
e) Geração e armazenamento de registros de auditoria da ACPR;
f) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
g) 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 reside é inspecionado. Todo equipamento que deixar de ser utilizado em caráter permanente terão suas informações sensíveis relativas à atividade da ACPR destruídas de maneira definitiva. Todos esses eventos são registrados para fins de auditoria.

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

6.5.2 Classificação da segurança computacional

A ACPR aplica configurações de segurança definida como EAL3, baseada na “Common Criteria” e desenvolvida para o sistema operacional SUSE LINUX pela SUSE, que disponibiliza as atualizações deste sistema operacional utilizado nos servidores do Sistema de Certificação Digital do prestador de Serviço de Suporte da ACPR.

6.5.3 Controle de segurança para as Autoridades de Registro

São os itens aplicáveis descritos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistemas

6.6.1.1. A ACPR adota o Sistema de Certificação Digital do SERPRO (Serviço Federal de Processamento de Dados), desenvolvido em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e depois de concluído os testes é colocado em um ambiente de homologação. Finalizado o processo de homologação das customizações, o Gerente do Prestador de Serviço de Suporte avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2 Controle de gerenciamento de segurança

6.6.2.1. Os níveis de segurança empregados pela ACPR e AR são controlados pelos privilégios nomeados a contas de sistema operacional e pelos papéis confiados descritos no item 5.2.1.

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

a) Instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
b) Implantação ou modificação de Autoridades Certificadoras com customizações a nível de certificados, páginas web, scripts, etc.;
c) Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e
d) Instalação de novos serviços na plataforma de processamento.

6.6.3 Classificação de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração de LCR

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

6.7 Controles de Segurança de Rede

6.7.1 Diretrizes Gerais.

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

a) Os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), que atendem o segmento de rede dos servidores web do sistema de certificação da ACPR estão localizados e operam em ambiente protegido por três perímetros de segurança: os dois primeiros controlados por vigilantes e o terceiro constituído por controle de acesso biométrico;
b) As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (patches), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento e homologação;
c) 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 permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo;
d) Infraestrutura de conectividade, incluindo:
    - alojamento seguro de equipamento de comunicação;
    - firewall seguro e serviços de roteador;
    - serviço de LAN seguro;
    - serviço back office seguro;
    - serviço de internet seguro e redundante.
e) Prevenção incidente e avaliação, incluindo,
    - descoberta de intrusão;
    - análise de vulnerabilidade;
    - configuração segura de servidor;
    - auditorias técnicas.
    - administração de infraestrutura, incluindo
    - monitoramento de servidor;
    - monitoramento de rede;
    - monitoramento de URL;
    - relatórios de largura da banda.

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

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

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

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

6.7.2 Firewall

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

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

6.7.3 Sistema de detecção de intrusão (IDS)

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

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

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

6.7.4 Registro de acessos não autorizados à rede

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

6.8 Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela ACPR para o armazenamento de sua chave privada implementa as características de segurança do padrão Homologação da ICP-Brasil NSH-3, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

7. PERFIS DE CERTIFICADO E LCR

7.1 Diretrizes Gerais

7.1.1. Nos seguintes itens são descritos os aspectos dos certificados e LCR emitidos sob esta DPC.

7.1.2. A Política de Certificado abaixo especifica o formato do certificado gerado e das correspondentes LCR. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

- Política de Certificado A3 da ACPR para Certificação de Pessoa Física e Pessoa Jurídica - PC A3 ACPR, OID 2.16.76.1.2.3.1.

7.1.3. Não se aplica.

7.2 Perfil do Certificado

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

7.2.1 Número(s) de versão

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

7.2.2 Extensões de certificados

A ACPR não emite certificados de AC

7.2.3 Identificadores de algoritmos

A ACPR não emite certificados de AC

7.2.4 Formatos de nome

A ACPR não emite certificados de AC

7.2.5 Restrições de nome

A ACPR não emite certificados de AC

7.2.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a ACPR após conclusão do processo de seu credenciamento, é **2.16.76.1.1.1**.

7.2.7 Uso da extensão "Policy Constraints"

Não se aplica.

7.2.8 Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web http://repositorio.serpro.gov.br/docs/dpcacpr.pdf da DPC ACPR em vigor.

7.2.9 Semântica de processamento para extensões criticas

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

7.3 Perfil de LCR

7.3.1 Número (s) de versão

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

7.3.2 Extensões de LCR e de suas entradas

7.3.2.1. A ACPR adota as seguintes extensões de LCR:

a) **"Authority Key Identifier", não crítica**: contém o *hash* SHA-1 da chave pública da ACPR que assina a LCR;
b) **"CRL Number", não crítica**: contém número sequencial para cada LCR emitida;
c) **"Authority Information Access", não crítica**: contém somente o método de acesso id-ad-calssuer, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação. Não é utilizado nenhum outro método de acesso diferente de id-ad-calssuer.

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

a) ***"Autority Key Identifier",* não crítica***:* deve conter o *hash SHA-1* da chave pública da AC que assina a LCR; e
b) ***"CRL Number",* não crítica**: deve conter um número sequencial para cada LCR emitida pela AC.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 Procedimentos de mudança de especificação

Qualquer alteração nesta DPC da ACPR será submetida previamente à aprovação do CG da ICP-Brasil. A DPC será alterada sempre que uma nova PC implementada o exigir.

8.2 Políticas de publicação e de notificação

A ACPR publica esta DPC, em sua página *web* acessível pela URL http://repositorio.serpro.gov.br/docs/dpcacpr.pdf. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na *web*.

8.3 Procedimentos de aprovação

Todas as DPC no âmbito da ICP-Brasil são submetidas à aprovação durante o processo de credenciamento da ACPR*,* conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9. DOCUMENTOS REFERENCIADOS

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

Ref	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

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

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

9.3. O documento abaixo é aprovado pela AC Raiz, podendo ser alterado, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br/.

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