www.serpro.gov.br

Declaração de Práticas de Certificação
da
Autoridade Certificadora
do SERPRO

(DPC ACSERPRO)

Versão 4.0 de 01/06/2011

Controle de Versão

Versão	Data	Motivo	Descrição
1.0	16/09/2005	Criação	Versão inicial
2.0	26/06/2006	Alteração	Adequações às Resoluções da ICP-Brasil
3.0	15/12/2008	Alteração	Adequações determinadas na Resolução 48 de 03/12/2007: inclusão do item 3.1.1.5, 6.6.4 e alteração no item 3.1.10.2; Aumenta o número máximo de custodiantes da chave de ativação da AC de 9 para 15 (item 6.2.2, 6.2.7 e 6.2.8); Utilização do sistema de AC Ywyra (itens 4.5.6, 6.1.1.2, 6.1.8.1, 6.2, 6.5.2, 6.6.1 e 6.8) Renovação da ACSERPRO (novo endereço da LCR – item 7.2.2);
4.0	01/06/2011	Alteração	Atualizações de acordo com DOC-ICP-05 versão 3.5 e criação da ACSERPRO v3 sob a cadeia da AC Raiz v2: 1.3.2.1, 2.1.1, 2.2.1.3, 2.5, 3.1.1.5, 3.1.1.6, 3.2.2, 4.1.1, 4.4.9.1, 4.4.15.2, 4.5.1.7, 4.6.2, 6.1.1.1, 6.1.4, 6.1.5.2, 6.1.6, 6.1.8.1, 6.1.9.1, 6.2, 6.2.1.1, 6.3.2.4, 6.8, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.2.9, 7.3.1, 7.3.2, 8.1 e 9.3.

SUMÁRIO

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
ACT – Autoridade de Carimbo de Tempo
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 - Infra-Estrutura 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
SINRIC – Sistema Nacional de Registro de Identificação Civil
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 Este documento estabelece os requisitos mínimos a serem obrigatoriamente observados pela ACSERPRO, integrante da Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de sua Declaração de Práticas de Certificação – DPC. Esta DPC descreve as práticas e os procedimentos empregados pela Autoridade Certificadora do SERPRO, ACSERPRO, na execução dos seus serviços.

1.1.2 Toda DPC elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada no documento DOC-ICP-05.

1.2 IDENTIFICAÇÃO

Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO”, integrante da ICP-Brasil e comumente referida como “DPC ACSERPRO”. O Identificador de Objeto **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.2**.

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 Autoridades Certificadoras

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

1.3.2 Autoridades de Registro

1.3.2.1 A Autoridade de Registro credenciada pela AC SERPRO é a AR SERPRO, responsável pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes. O endereço da página web (URL) da ACSERPRO é https://ccd.serpro.gov.br/acserpro.

1.3.2.2 A ACSERPRO mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A ACSERPRO não publica em sua página https://ccd.serpro.gov.br/acserpro a relação de prestadores de serviço de suporte, pois não utiliza este recurso em suas operações;

1.3.3.2 PSS são entidades utilizadas pela AC ou pela AR para desempenhar as atividades descritas abaixo:

a) Disponibilização de infra-estrutura física e lógica;
b) Disponibilização de recursos humanos especializados; ou
c) Disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.3.3 A ACSERPRO mantém as informações acima atualizadas.

1.3.4 Titulares de Certificado

A ACSERPRO emite certificados para Autoridades Certificadoras de nível imediatamente subseqüente ao seu.
Os titulares dos certificados são as entidades pessoas jurídicas, autorizadas pela AR da ACSERPRO a receberem certificados digitais emitidos pela ACSERPRO, e credenciadas pela AC Raiz para integrar a ICP-Brasil.

1.3.5 Aplicabilidade

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

1.4 DADOS DE CONTATO

Esta DPC é administrada pelo Centro de Certificação Digital do SERPRO, CCD-SERPRO, localizado no seguinte endereço:

SGAN 601 Módulo V
Bairro: Asa Norte
CEP: 70.836-900
Brasília / DF.

Pessoas de Contato.

Nome: Gilberto de Oliveira Netto
Telefone: (61) 2021-8651
Fax: (61) 2021-8516
(encaminhar aos cuidados do CCD SERPRO)

E-mail de Contato.

ccdserpro@serpro.gov.br

2. DISPOSIÇÕES GERAIS

2.1 OBRIGAÇÕES E DIREITOS

2.1.1 Obrigações da ACSERPRO

As obrigações da ACSERPRO são as abaixo relacionadas:

a) Operar de acordo com esta DPC;

b) Gerar e gerenciar o seu par de chaves criptográficas;

c) Assegurar a proteção de sua chave privada;

d) Notificar a AC Raiz da ICP-Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;

e) Notificar as AC de nível imediatamente subseqüente ao seu quando ocorrer suspeita de comprometimento de sua chave, 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 das AC de nível imediatamente subseqüente ao seu.

h) Informar a emissão do certificado ao respectivo solicitante;

i) Revogar os certificados por ela emitidos;

j) Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);

k) Publicar em sua página *web* a DPC ACSERPRO aprovada e implementada;

l) Publicar em sua página *web* as informações definidas no item 2.6.1.2 desse documento;

m) Publicar, em página web, informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;

n) Utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;

o) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

p) Adotar as medidas de segurança e controle previstas nesta DPC e na Política de Segurança que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios e procedimentos da ICP-Brasil;

q) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

r) Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

s) Manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;

t) Manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas AC de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;

u) Informar as terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC;

v) Informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos; e

w) Não emitir certificados com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações da AR SERPRO

As obrigações da AR SERPRO 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 ACSERPRO 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 ACSERPRO aos seus respectivos solicitantes;

f) Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasi;

g) Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela ACSERPRO, 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; e

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 do titular de certificado emitido de acordo com esta DPC ACSERPRO são as abaixo relacionadas:

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 suas respectivas chaves privadas de modo apropriado, conforme o previsto nesta DPC;

d) Conhecer os seus direitos e obrigações, contemplados pela DPC da ACSERPRO e por outros documentos aplicáveis da ICP-Brasil; e

e) Informar à ACSERPRO qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;

NOTA: Em se tratando de certificado emitido para AC (Órgãos públicos ou pessoas jurídicas), 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 nesta DPC;

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

i. não constar da LCR da ACSERPRO;

ii. não estiver expirado; e

iii. puder ser verificado com o uso de certificado válido da ACSERPRO;

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

2.1.5 Obrigações do Repositório

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela ACSERPRO e a sua LCR;

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

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

2.2 RESPONSABILIDADES

2.2.1 Responsabilidades da ACSERPRO

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

2.2.1.2. A ACSERPRO responde solidariamente pelos atos das entidades de sua cadeia de certificação: AC subordinadas, AR e PSS.

2.2.1.3. Não se aplica.

2.2.2 Responsabilidades da AR

A AR SERPRO 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

A ACSERPRO ou a AR SERPRO indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3 Processos Administrativos

Será seguida legislação específica uma vez que a ACSERPRO é administrada pelo Serviço Federal de Processamento de Dados – SERPRO, empresa vinculada ao Ministério da Fazenda.

2.4 INTERPRETAÇÃO E EXECUÇÃO

2.4.1 Legislação

A DPC ACSERPRO obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil. Além disto, é apoiada em uma estrutura contratual entre SERPRO e Titulares de Certificados.

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, o corpo técnico da ACSERPRO examinará a disposição inválida e proporá à Comissão Técnica, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada. As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

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

2.4.3 Procedimentos de solução de disputa

2.4.3.1 No caso de um conflito entre esta DPC e outras declarações, políticas, planos, acordos, contratos ou documentos que a ACSERPRO adotar, nesta situação esta DPC prevalecerá.

2.4.3.2 No caso de um conflito entre esta DPC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre 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

As tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu podem ser consultadas através de solicitação à caixa postal indicada no item 1.4 desta DPC.

2.5.1 Tarifas de emissão e renovação de certificados

As tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu podem ser consultadas através de solicitação à caixa postal indicada no item 1.4 desta DPC.

2.5.2 Tarifas de acesso ao certificado

As tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu podem ser consultadas através de solicitação à caixa postal indicada no item 1.4 desta DPC.

2.5.3 Tarifas de revogação ou de acesso à informação de status

As tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu podem ser consultadas através de solicitação à caixa postal indicada no item 1.4 desta DPC.

2.5.4 Tarifas para outros serviços

As tarifas previstas pela ACSERPRO para os serviços prestados às AC de nível imediatamente subseqüente ao seu podem ser consultadas através de solicitação à caixa postal indicada no item 1.4 desta DPC.

2.5.5 Política de reembolso

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

2.6 PUBLICAÇÃO E REPOSITÓRIO

2.6.1 Publicação de informação da ACSERPRO

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

2.6.1.2 As seguintes informações são publicadas na página web da ACSERPRO:

a) O certificado da ACSERPRO;
b) sua LCR;
c) esta DPC e a PC que implementa;
d) os certificados das AC de nível imediatamente subseqüente ao seu;
e) a AR vinculada e seu respectivo endereço de instalação técnica em funcionamento;

2.6.2 Freqüência de publicação

Os certificados e a LCR são publicados imediatamente após sua emissão pela ACSERPRO. As demais informações mencionadas no item 2.6.1 serão publicadas sempre que sofrerem alterações.

2.6.3 Controles de acesso

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

incluirão identificação pessoal para acesso aos equipamentos com utilização de senhas fortes.

2.6.4 Repositórios

A ACSERPRO utiliza sua página web como repositório das informações que publica, e atende aos seguintes requisitos:

a) localização: https://ccd.serpro.gov.br/acserpro/,
b) disponibilidade: aquela definida no item 2.6.1.1 desta DPC;
c) protocolos de acesso: HTTP e HTTPS;
d) requisitos de segurança: obedece aos requisitos definidos no item 5 desta DPC ACSERPRO.

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 ACSERPRO estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.2. As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu 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, a auditoria da ACSERPRO 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 ACSERPRO informa que recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e que é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, freqüência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5. A ACSERPRO informa que as entidades da ICP-Brasil a ela diretamente vinculadas – AC, AR e PSS, também receberam auditoria prévia, para fins de credenciamento, e que a AC é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8 SIGILO

2.8.1 Disposições Gerais

2.8.1.1 A chave privada de assinatura digital da ACSERPRO foi gerada e é mantida pela própria ACSERPRO, 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 ACSERPRO, 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 ACSERPRO não emite certificados de sigilo.

2.8.2Tipos de informações sigilosas

2.8.2.1 Todas as informações coletadas, geradas, transmitidas e mantidas pela ACSERPRO e a AR SERPRO 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 à ACSERPRO ou AR SERPRO deverá ser divulgado.

2.8.3 Tipos de informações não sigilosas

Os seguintes documentos da ACSERPRO e AR SERPRO 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 pela AC;
d) a DPC da AC;
e) versões públicas de Políticas de Segurança; e
f) a conclusão dos relatórios de auditoria.

2.8.4 Divulgação de informação de revogação/suspensão de certificado

2.8.4.1. A ACSERPRO divulga informações de revogação de certificados por ela emitidos, inclusive as razões para a revogação, na sua página web descrita no item 2.6.1 desta DPC, através de sua lista de certificados revogados.

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

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

2.8.5 Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da ACSERPRO e AR SERPRO é divulgado a entidades legais ou seus funcionários, exceto quando:

a) Exista uma ordem judicial corretamente constituída; e
b) Esteja corretamente identificado o representante da lei.

2.8.6 Informações a terceiros

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

2.8.7 Divulgação por solicitação do titular

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

2.8.7.2. Qualquer liberação de informação pela ACSERPRO ou AR SERPRO, somente será permitida mediante autorização formal do titular do certificado. As formas de autorização são as seguintes:

a) por meio eletrônico, contendo assinatura válida garantida por certificado do titular, reconhecido pela ACSERPRO; ou
b) por meio de pedido escrito com firma reconhecida.

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

Todos os direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, e todos os documentos gerados para a ACSERPRO (eletrônicos ou não), de acordo com a legislação vigente, pertencem e continuarão sendo propriedade do Serviço Federal de Processamento de Dados – SERPRO.

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 SERPRO, vinculada à ACSERPRO, 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 de pessoa física é realmente aquela cujos dados constam na documentação apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil;

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;

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, observando que deve ser executada, obrigatoriamente:

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

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

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

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

.

3.1.1.2. O processo de validação poderá ser realizado pelo agente de registro fora do ambiente físico da AR, desde que utilizado ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR.

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

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

3.1.1.5. Não se aplica.

3.1.1.6. Não se aplica.

3.1.2 Tipos de nomes

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

3.1.2.2. A ACSERPRO não inclui no certificado das AC subseqüentes o nome da pessoa física responsável pelo mesmo.

3.1.3 Necessidade de nomes significativos

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

3.1.4 Regras para interpretação de vários tipos de nomes

Item não aplicável.

3.1.5 Unicidade de nomes

Os identificadores "*Distinguished Name*" (DN) são únicos para cada AC de nível imediatamente subseqüente ao da ACSERPRO. Para cada AC, números ou letras

adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509.

3.1.6 Procedimento para resolver disputa de nomes

A ACSERPRO reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes das AC de nível imediatamente subseqüente ao seu. Durante o processo de confirmação de identidade, a AC solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

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

A confirmação que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, 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.

3.1.9.1. Documentos para efeito de identificação de um indivíduo

As solicitações de certificados, para as AC subordinadas, devem ser realizadas por pessoa física legalmente responsável, que deverá apresentar a seguinte documentação, em sua versão original:

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) caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos, ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data de validação presencial;
e) comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data de validação presencial.

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.
NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.
NOTA 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.9.2.1. Não se aplica.

3.1.9.2.2. Não se aplica.

3.1.9.2.3. Não se aplica.

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, devendo a cópia da mesma 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 SERPRO para a confirmação da identidade de uma AC subordinada é feita mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

3.1.10.1.2. A pessoa física, responsável legal da AC subordinada, será identificada na forma descrita no item 3.1.9.1 deste documento.

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.

NOTA: A AC subordinada solicitante será obrigatoriamente identificada pela AC Raiz, por intermédio da ACSERPRO, por meio dos procedimentos descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

3.1.10.2. Documentos para efeitos de identificação de uma organização

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

a) Relativos a sua habilitação jurídica:

i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;

ii. se entidade privada:

1. ato constitutivo, devidamente registrado no órgão competente; e

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

b) Relativos a sua habilitação fiscal:

i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ; ou

ii. prova de inscrição no Cadastro Específico do INSS – CEI.

3.1.10.3. Informações contidas no certificado emitido para uma organização

Não se aplica.

3.1.11 Autenticação da Identidade de um equipamento ou aplicação

Não se aplica.

3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

3.2.1. O processo de identificação do solicitante quando da geração de novo par de chaves e emissão pela ACSERPRO de novo certificado, antes da expiração do atual, será o mesmo da primeira emissão.

3.2.2. Esse processo será conduzido da seguinte forma:

a) Adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;

b) Não se aplica;

c) Em caso de pessoa jurídica, qualquer alteração em sua constituição e funcionamento deverá constar do processo de renovação.

3.2.3. Não se aplica.

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 ACSERPRO de novo certificado, após expiração ou revogação do anterior, será o mesmo da primeira emissão.

3.3.2. Após a expiração ou revogação de seu certificado, uma AC deve executar os processos regulares de geração de novo par de chaves.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado de AC imediatamente subseqüente será feita formalmente pelo representante legal da AC imediatamente subseqüente, e com a presença física do mesmo, a fim de possibilitar a sua identificação inequívoca.

4. REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

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

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

2) Assinatura do Termo de Titularidade;

4.1.2. A solicitação de certificado para AC de nível imediatamente subseqüente ao da ACSERPRO somente é possível após o deferimento do pedido de credenciamento e a respectiva autorização de funcionamento da AC em questão pela AC-Raiz, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.3. Nesse caso, a AC subsequente deve encaminhar a solicitação de seu certificado à ACSERPRO por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

4.2 EMISSÃO DE CERTIFICADO

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

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

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

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

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

4.3 ACEITAÇÃO DE CERTIFICADO

4.3.1. O processo de aceitação de um certificado emitido pela ACSERPRO a uma AC subsequente se dará em duas etapas: na cerimônia de emissão do certificado,

perante os representantes legais da mesma, e após sua utilização no ambiente operacional da AC Subsequente.

4.3.2. A AC de nível imediatamente subseqüente irá declarar, através de seus representantes legais, mediante assinatura do "Termo de Acordo", que aceita o certificado emitido. A aceitação implica que o solicitante reconhece a veracidade dos dados contidos no certificado.

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

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 Circunstâncias para revogação

4.4.1.1. Um certificado de AC de nível imediatamente subseqüente ao da ACSERPRO pode ser revogado a qualquer momento nas seguintes circunstâncias: por solicitação da AC titular do certificado, por decisão da ACSERPRO , do CG da ICP-Brasil ou da AC Raiz.

4.4.1.2. Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

a) quando constatada emissão imprópria ou defeituosa;
b) quando for necessária a alteração de qualquer informação constante no mesmo;
c) no caso de dissolução da AC titular do certificado; ou
d) no caso de perda, roubo, modificação, acesso indevido ou 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 ACSERPRO 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; e
b) 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 revogação do certificado de uma AC de nível imediatamente subseqüente ao da ACSERPRO somente pode ser feita:

a) pela AC Titular do Certificado;
b) pela ACSERPRO;
c) pela AR-SERPRO;
d) pelo CG da ICP-Brasil;
e) pela AC Raiz;

4.4.3 Procedimento para solicitação de revogação

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

4.4.3.2. Como diretrizes gerais, fica estabelecido que:

a) O solicitante da revogação de um certificado deve ser identificado;
b) As solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;
c) As justificativas para a revogação de um certificado são documentadas; e
d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.4.3.3. Não se aplica.

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

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

4.4.3.6. 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. A AC subsequente poderá solicitar a revogação de seu certificado e nova emissão sem ônus, no período correspondente entre a emissão e a aceitação definitiva do mesmo, definida no item 4.3.

4.4.4.2. Não se aplica.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

4.4.9 Freqüência de emissão de LCR

4.4.9.1. A ACSERPRO emite a LCR referente a certificados de AC subordinadas em um prazo máximo de 45 (quarenta e cinco) dias.

4.4.9.2. Não se aplica.

4.4.9.3. A freqüência máxima admitida para a emissão de LCR referentes a certificados de AC é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a ACSERPRO emitirá nova LCR no prazo previsto no item 4.4.3 e notificará todas as AC de nível imediatamente subsequente ao seu.

4.4.9.4. Não se aplica

4.4.10 Requisitos para verificação de LCR

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

4.4.10.2. A autenticidade da LCR deve também ser confirmada por meio da verificação da assinatura da ACSERPRO e do período de validade da LCR.

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

A ACSERPRO não disponibiliza recursos para revogação ou verificação *on-line* de estado de certificados.

4.4.12 Requisitos para verificação de revogação *on-line*

A ACSERPRO não disponibiliza diretório *on-line* ou um servidor de OCSP para verificar o estado dos certificados emitidos pela ACSERPRO.

4.4.13 Outras formas disponíveis para divulgação de revogação

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

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. No caso do comprometimento da chave privada de uma AC de nível imediatamente subseqüente ao da ACSERPRO, a mesma deve notificar imediatamente à ACSERPRO, solicitando a revogação de seu certificado,

conforme descrito no item 4.4.3 desta DPC.

4.4.15.2. A ACSERPRO disponibiliza seus dados de contato no item 4.1 desta DPC para a comunicação do comprometimento da chave de AC subsequente.

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 ACSERPRO, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A ACSERPRO registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

a) Iniciação e desligamento do sistema de certificação;
b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACSERPRO;
c) Mudanças na configuração da ACSERPRO 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 ACSERPRO 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; e
l) Operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A ACSERPRO registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, quais sejam:

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

4.5.1.3. Os registros de auditoria mínimos a serem mantidos pela ACSERPRO 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 ACSERPRO é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil.

4.5.1.6. Não se aplica.

4.5.1.7. A ACSERPRO define que o local de arquivamento das cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados, e dos termos de titularidade é o mesmo das instalações de contingência da ACSERPRO.

4.5.2 Freqüência de auditoria de registros (*logs*)

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

Os registros de auditoria são analisados pelo pessoal operacional da ACSERPRO. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros verificando-se que não foram alterados, em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3 Período de Retenção para registros (*logs*) de Auditoria

A ACSERPRO mantém localmente, nas instalações do SERPRO, os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, 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 eletrônicamente 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.

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.

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 ACSERPRO executa procedimentos de backup de todo o sistema de certificação, sempre que houver utilização do mesmo, seguindo scripts previamente desenvolvidos para estas atividades.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da ACSERPRO é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de ACSERPRO, pelo sistema de controle de acesso e pelo pessoal operacional.

4.5.7 Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da ACSERPRO 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 ACSERPRO, 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 ACSERPRO:

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 ACSERPRO; e
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 LCRs e os certificados de assinatura digital deverão ser retidos

permanentemente, para fins de consulta histórica;

b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. **As prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado;** e

c) as demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 6 (seis) 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 ACSERPRO, e recebem o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

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

4.6.5 Requisitos para datação de registros

Os servidores da ACSERPRO 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.
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 ACSERPRO 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/ARe 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

A integridade dos arquivos da ACSERPRO e da AR-SERPRO é verificada:

- Na ocasião em que o arquivo é preparado;
- Semestralmente no momento de uma auditoria de segurança programada;
- Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

4.7 TROCA DE CHAVE

4.7.1. A ACSERPRO comunica através de oficio, com 90 dias de antecedência, à AC subseqüente o vencimento do seu certificado, junto com as informações necessárias para a solicitação de uma nova chave.

4.7.2. Não se aplica.

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

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

4.8.1 Recursos computacionais, *software* e dados corrompidos

A ACSERPRO 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 ACSERPRO.

4.8.2 Certificado de entidade é revogado

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que o certificado da ACSERPRO é revogado, e que podem ser resumidas da seguinte forma:

a) Em caso de revogação do certificado da ACSERPRO, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados das AC de nível imediatamente subseqüente, é gerado o novo par de chaves da ACSERPRO, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela ACSERPRO, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.3 Chave de entidade é comprometida

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que a chave privada da ACSERPRO é comprometida, e que podem ser resumidas nas ações listadas a seguir:

a) Em caso de comprometimento da chave da ACSERPRO, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da ACSERPRO e das AC de nível imediatamente subseqüente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela ACSERPRO, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

A ACSERPRO 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 ACSERPRO quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.
O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a ACSERPRO faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a ACSERPRO para tornar acessível os registros lógicos mantidos dentro do *software*. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

4.8.5 Atividades das Autoridades de Registro

Não se aplica.

4.9 EXTINÇÃO DOS SERVIÇOS DA AC, AR OU PSS

4.9.1. A ACSERPRO observa os procedimentos descritos no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

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

a) Prover com maior antecedência possível notificação para:
b) a AC Raiz da ICP-Brasil;
c) todas as entidades subordinadas.
d) A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a ACSERPRO ou para a AR-SERPRO extinta;
e) Preservar qualquer registro não transferido a um sucessor.
f) As chaves públicas dos certificados emitidos pela ACSERPRO, dissolvida, serão armazenadas por outra AC, após aprovação da AC Raiz.
g) Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela ACSERPRO.
h) A ACSERPRO, 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.
i) 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 AC responsável pela DPC 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 ACSERPRO 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 ACSERPRO, 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 ACSERPRO 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 ACSERPRO, 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 ACSERPRO. 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 ACSERPRO transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da ACSERPRO 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 ACSERPRO, 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 ACSERPRO. 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 ACSERPRO. 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 ACSERPRO, 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 ACSERPRO, tais como: emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

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

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

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

- Sala de equipamentos de produção *on-line* e cofre de armazenamento;
- Sala de equipamentos de produção *off-line* e cofre de armazenamento; e
- Equipamentos de rede e infra-estrutura (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:

- Ser feito em aço ou material de resistência equivalente; e
- 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 ACSERPRO 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 ACSERPRO 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 infra-estrutura do ambiente de certificação da ACSERPRO 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

ACSERPRO 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 à falhas.

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

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

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC 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 ACSERPRO não é permitido fumar ou portar objetos que produzam fogo ou faísca.

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

5.1.5.4. Em caso de incêndio nas instalações da ACSERPRO, 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 ACSERPRO 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 ténicas de AR

As instalações técnicas da AR-SERPRO atendem aos requisitos estabelecidos no documento CARACTERISTICAS 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 ACSERPRO, 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 empregada estão limitadas de acordo com o seu perfil.

5.2.1.2. A ACSERPRO 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 ACSERPRO 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. 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 ACSERPRO, conforme o descrito em 6.2.2.

5.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da ACSERPRO necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da ACSERPRO. As demais tarefas da ACSERPRO 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 ACSERPRO passam por um processo rigoroso de seleção.

Todo funcionário da ACSERPRO tem sua identidade e perfil verificados antes de:

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

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 ACSERPRO devidamente qualificado);
b) Não são compartilhados;
c) São restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3 A ACSERPRO 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], juntamente com procedimentos de validação dessas senhas.

5.3 CONTROLES DE PESSOAL

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela ACSERPRO, 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. A DPC garante que todos os empregados da ACSERPRO 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 ACSERPRO;
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 ACSERPRO e AR SERPRO 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 ACSERPRO 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 ACSERPRO, 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 ACSERPRO poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal da ACSERPRO 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 ACSERPRO e das AR vinculadas;
b) Sistema de certificação em uso na ACSERPRO;
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
e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Freqüência e requisitos para reciclagem técnica

Todo o pessoal da ACSERPRO e das ARs 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 ACSERPRO. Treinamentos de reciclagem são realizados pela ACSERPRO sempre que necessário.

5.3.5 Freqüência e seqüência de rodízios de cargos

A ACSERPRO não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

5.3.6.1. A ACSERPRO, na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da ACSERPRO ou de uma AR vinculada, suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação, 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
e) conclusões.

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

5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:
a) advertência;
b) suspensão por prazo determinado; ou
c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 Requisitos para contratação de pessoal

O pessoal da ACSERPRO 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 ACSERPRO disponibiliza para todo o seu pessoal, para a AR vinculada:

a) Esta DPC;
b) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8];
c) A Política de Segurança da ACSERPRO;
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 ACSERPRO é gerado pela própria ACSERPRO, em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], padrão "Homologação da ICP-Brasil NSH-3", após o deferimento do pedido de credenciamento da mesma e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. O par de chaves criptográficas de uma AC de nível imediatamente subseqüente ao da ACSERPRO é gerado pela própria AC, após o deferimento do pedido de credenciamento e habilitação da mesma, e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil. Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]. A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento. O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada é única e seu sigilo é suficientemente assegurado;
b) a chave privada não pode, com uma segurança razoável, ser deduzida;
c) a chave privada está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
d) a chave privada pode ser eficazmente protegida pelo legítimo titular contra

a utilização por terceiros;

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.

6.1.1.3. Não se aplica.

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

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

6.1.4 Disponibilização de chave pública da ACSERPRO para usuários

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

a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9];
b) Diretório;
c) Página *web* da ACSERPRO (http://ccd.serpro.gov.br/acserpro/);
d) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1. Não se aplica.

6.1.5.2. O tamanho das chaves criptográficas associadas a certificados emitidos pela ACSERPRO será de 4096 (quatro mil e noventa e seis) bits para a AC SERPRO V3 e de 2048 (dois mil e quarenta e oito) bits para as AC SERPRO V1 e V2, conforme estabelecido para chaves criptográficas associadas a certificados de AC, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da ACSERPRO seguem o padrão "Homologação da ICP-Brasil NSH-3", definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7 Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave segue o padrão "Homologação da ICP-Brasil NSH-3", 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 da ACSERPRO é feito por hardware criptográfico com padrão de segurança "Homologação da ICP-Brasil NSH-3", definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8.2. Não se aplica.

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

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

6.1.9.2 A chave privada da ACSERPRO 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 ACSERPRO 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 ACSERPRO adota o padrão "Homologação da ICP-Brasil NSH-3", definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

6.2.2 Controle 'n de m' para chave privada

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

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

6.2.3 Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, Isto é, não se permite que terceiros possam legalmente obter uma chave privada com 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 ACSERPRO mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.

6.2.4.3. A ACSERPRO não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.

6.2.4.4. A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+, ou outros definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

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

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

6.2.6 Inserção de chave privada em módulo criptográfico

A chave privada da ACSERPRO 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 ACSERPRO é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de "n" de "m" dos *custodiantes* da chave de ativação da chave criptográfica, na quantidade definida no item 6.2.2. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da

ACSERPRO. As senhas utilizadas obedecem à política de senhas estabelecida pela ACSERPRO.

6.2.8 Método de desativação de chave privada

A chave privada da ACSERPRO, 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 "n" de "m" dos *custodiantes* da chave de ativação da chave criptográfica, na quantidade definida no item 6.2.2. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da ACSERPRO. As senhas utilizadas obedecem à política de senhas estabelecida pela ACSERPRO.

6.2.9 Método de destruição de chave privada

Quando a chave privada da ACSERPRO for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, deve ser sobrescrito. Todas as cópias de segurança da chave privada da ACSERPRO 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 ACSERPRO.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

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

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1. A chave privada da ACSERPRO e dos titulares de certificados por ela emitidos será utilizada apenas durante o período de validade dos certificados correspondentes. A chave pública da ACSERPRO 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. Os certificados emitidos pela ACSERPRO para as AC de nível imediatamente subseqüente ao seu terão validade de no máximo 8 (oito) anos.

6.3.2.4. O período de validade do certificado da ACSERPRO é de 10 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.

6.4.1 Geração e instalação dos dados de ativação

6.4.1.1. A ACSERPRO 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 ACSERPRO garante que a geração de seu par de chaves é realizada em ambiente *off-line,* para impedir o acesso remoto não autorizado.
6.5.1.2. Os requisitos gerais de segurança computacional dos equipamentos utilizados para a geração dos pares de chaves criptográficas das AC titulares de certificados emitidos pela ACSERPRO, devem ser os mesmos descritos no item abaixo para os computadores servidores da ACSERPRO.

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

a) Controle de acesso aos serviços e perfis da ACSERPRO;

b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da ACSERPRO;
c) Acesso restrito aos bancos de dados da ACSERPRO;
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 ACSERPRO;
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 residem os equipamentos utilizados para operação da ACSERPRO ou da AC subordinada, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da ACSERPRO ou AC subseqüente. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à ACSERPRO, 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 ACSERPRO aplica configurações de segurança definida como **EAL3 Evaluated Configuration Guide for Red Hat Enterprise Linux**, baseada na Common Criteria, que disponibiliza as atualizações deste sistema operacional utilizado nos servidores do Sistema de Certificação Digital utilizado no SERPRO.

6.5.3 Controle de segurança para as Autoridades de Registro

6.5.3.1. Não se aplica.
6.5.3.2. Não se aplica.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 Controles de desenvolvimento de sistemas

6.6.1.1. A ACSERPRO adota o Sistema de Certificação Digital Ywyra, desenvolvido em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluído os testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das

customizações, o Gerente do CCD avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2 Controle de gerenciamento de segurança

6.6.2.1. As ferramentas e os procedimentos empregados pela ACSERPRO para garantir que os seus sistemas implementem os níveis configurados de segurança são os seguintes:

a) A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.
b) A ACSERPRO opera em equipamento off-line, portanto não necessita configuração de segurança de rede.

6.6.2.2. O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela ACSERPRO, 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

Este item não se aplica.

6.6.4 Controles na Geração de LCR

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

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 Diretrizes Gerais

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

a) Os servidores e elementos de infra-estrutura 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 ACSERPRO, 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) Acesso lógico aos elementos de infra-estrutura 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) Infra-estrutura de conectividade, incluindo:
   i. alojamento seguro de equipamento de comunicação;
   ii. firewall seguro e serviços de roteador;
   iii. serviço de LAN seguro;
   iv. serviço back office seguro; e
   v. serviço de internet seguro e redundante.

e) Prevenção incidente e avaliação, incluindo:
   i. descoberta de intrusão;
   ii. análise de vulnerabilidade;
   iii. configuração segura de servidor; e
   iv. auditorias técnicas.
   v. administração de Infra-estrutura, incluindo
   vi. monitoramento de servidor;
   vii. monitoramento de rede;
   viii. monitoramento de URL; e
   ix. relatórios de largura da banda.

6.7.1.2 Nos servidores e elementos de infra-estrutura e proteção de rede, utilizados pela ACSERPRO, somente os serviços estritamente necessários são habilitados.

6.7.1.3 Os servidores e elementos de infra-estrutura e proteção de rede tais como roteadores, hubs, switches, firewalls localizados no segmento de rede que

hospeda os servidores web do sistema de certificação da ACSERPRO, 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;

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 infra-estrutura 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).

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 responde-los automaticamente, com medidas tais como: enviar *traps SNMP*, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

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

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

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

O módulo criptográfico utilizado pela ACSERPRO 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].

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

a) a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
b) a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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 itens seguintes são descritos os aspectos dos certificados e LCR emitidos pela ACSERPRO.
7.1.2. Não se aplica.
7.1.3. A ACSERPRO especifica, nos itens seguintes, o formato dos certificados emitidos para as AC subsequentes.

7.2 PERFIL DO CERTIFICADO

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

7.2.2 Extensões de certificados

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

a) "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o *hash SHA-1* da chave pública da ACSERPRO;
b) S*ubject Key Identifier*", não crítica: contém o *hash SHA-1* da chave pública da AC titular do certificado;
c) K*ey Usage*", crítica: somente os bits e keyCertSign e cRLSign são ativados;
d) "Certificate Policies", não crítica:
   i. o campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;
   ii. o campo policyQualifiers contém o endereço *URL* da página *web, http://ccd.serpro.gov.br/acserpro/docs/dpcACSERPRO.pdf,* onde se obtém a DPC da ACSERPRO;
e) O "Basic Constraints", crítica: contém o campo CA=TRUE;
f) **CRLDistributionPoints:** contém o endereço na *Web* onde se obtém a LCR correspondente ao certificado:
   i. para certificados da cadeia ACSERPRO v1: http://ccd.serpro.gov.br/lcr/acserpro.crl;
   ii. para certificados da cadeia ACSERPRO V2: http://ccd.serpro.gov.br/lcr/acserprov2.crl;
   iii. para certificados da cadeia ACSERPRO V3: http://ccd.serpro.gov.br/lcr/acserprov3.crl e http://ccd2.serpro.gov.br/lcr/acserprov3.crl.

7.2.2.2 A ACSERPRO implementa as seguintes extensões, definidas como opcional pela ICP-Brasil, para os certificados emitidos sob a cadeia ACSERPRO v3.

a) "*Authority Information Access*", não critica, contendo o endereço na web onde se obtém o arquivo P7B com certificados da cadeia;
   - http://ccd.serpro.gov.br/cadeias/acserprov3.p7b
   - (OID = 1.3.6.1.5.5.7.1.1).

7.2.3 Identificadores de algoritmos

Os certificados emitidos pela ACSERPRO v3, sob a cadeia v2 da AC Raiz da ICP-Brasil, são assinados com o uso da suíte de assinatura sha512WithRSAEncryption, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

Os certificados emitidos pela ACSERPRO v1 e v2, sob as cadeias inicial e v1 da AC Raiz, foram assinados com o uso do algoritmo RSA com SHA-1 (OID = 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

7.2.4 Formatos de nome

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

C=BR
O= ICP-Brasil
OU= Servico Federal de Processamento de Dados – SERPRO
CN=nome da AC

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

C= BR
O= ICP-Brasil
OU= Servico Federal de Processamento de Dados – SERPRO
OU=CSPB-X *onde* "X" identifica a AC perante o SPB
CN= nome da AC

7.2.5 Restrições de nome

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

a) não serão utilizados sinais de acentuação, tremas ou cedilhas;
b) além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

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

7.2.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a ACSERPRO após conclusão do processo de seu credenciamento, é **2.16.76.1.1.2**.

7.2.7 Uso da extensão "Policy Constraints"

Não se aplica.

7.2.8 Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço *web* da DPC da ACSERPRO, http://ccd.serpro.gov.br/acserpro/docs/dpcACSERPRO*.pdf.*

7.2.9 Semântica de processamento para extensões criticas

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

7.3 PERFIL DE LCR

7.3.1 Número (s) de versão

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

7.3.2 Extensões de LCR e de suas entradas

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

7.3.2.2. As LCR da AC SERPRO obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões para certificados de AC:

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

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

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

8.2 POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO

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

8.3 PROCEDIMENTOS DE APROVAÇÃO

Essa DPC foi submetida à aprovação, durante o processo de credenciamento da ACSERPRO**,** 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 sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

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

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