Declaração de Práticas de Certificação da Autoridade Certificadora VALID. (DPC AC VALID).

[OID 2.16.76.1.1.43].
Versão 2.0 de 29/08/2016.

Conteúdo

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora

AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil

AR - Autoridades de Registro

CEI - Cadastro Específico do INSS

CG - Comitê Gestor

CMM-SEI - Capability Maturity Model do *Software* Engineering Institute

CMVP - Cryptographic Module Validation Program

CN - Common Name

CNE - Carteira Nacional de Estrangeiro

CNPJ - Cadastro Nacional de Pessoas Jurídicas

COBIT - Control Objectives for Information and related Technology

COSO - Comitee of Sponsoring Organizations

CPF - Cadastro de Pessoas Físicas

DMZ - Zona Desmilitarizada

DN - Distinguished Name

DPC - Declaração de Práticas de Certificação

ICP-Brasil - 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 - Online 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

PSBIO – Prestadores de Serviço Biométrico

PSS - Prestadores de Serviço de Suporte

RFC – Request For Comments

RG - Registro Geral

SNMP - Simple Network Management Protocol

TCSEC - Trusted System Evaluation Criteria

TSDM - Trusted *Software* Development Methodology

UF - Unidade de Federação

URL - Uniform Resource Location

1. INTRODUÇÃO

1.1. VISÃO GERAL

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

1.1.2. A AC VALID possui certificados de primeiro nível na ICP-Brasil assinados pela AC Raiz da ICP-Brasil. Os certificados da AC VALID contêm as chaves públicas correspondentes às chaves privadas utilizadas para assinar os certificados das ACs de nível imediatamente subsequente ao seu e as suas LCR (Lista de Certificados Revogados).

1.1.3. A AC VALID utiliza seu próprio ambiente para hospedar, operar e dar manutenção às suas atividades.

1.1.4. A estrutura desta DPC AC VALID está baseada nas resoluções do Comitê Gestor da ICP-Brasil (CG ICP-Brasil) e na RFC 2527 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Framework.

1.2. IDENTIFICAÇÃO

Este documento é chamado “Declaração de Práticas de Certificação da Autoridade Certificadora VALID” e comumente referido como “DPC AC VALID”. O Identificador de Objeto **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.43.**

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. Autoridades Certificadoras

Esta DPC refere-se unicamente à Autoridade Certificadora VALID (AC VALID) e encontra-se publicada no seu repositório, no seguinte endereço: http://icp-brasil.validcertificadora.com.br/ac-valid/dpc-ac-validv2.pdf

1.3.2. Autoridades de Registro

Os processos de identificação, cadastramento e recebimento de solicitações de renovação e revogação das ACs de nível imediatamente subsequente ao da AC VALID, são de competência de sua Autoridade de Registro vinculada, doravante chamada de AR VALID CERTIFICADORA DIGITAL OU AR VALID CD. A AC VALID disponibiliza e mantém atualizada na página http://www.validcertificadora.com.br as seguintes informações referentes à AR VALID CD:

a) o endereço de instalação da AR;

b) as pessoas e os meios para contato.

1.3.3. Prestador de Serviços de Suporte

A AC VALID utiliza o seguinte Prestador de Serviço de Suporte (PSS) nas suas operações:

- ✓ Valid Soluções e Serviços de Segurança em Meios de Pagamento e Identificação – PSS VALID S.A;
- ✓ Metrofile Brasil Gestão de Informática LTDA – PSS METROFILE.

1.3.4. Titulares de Certificado

A AC VALID emite certificados para Autoridades Certificadoras de nível imediatamente subsequente ao seu. Os titulares dos certificados são entidades e pessoas jurídicas de direito público e privado, autorizadas pela AR VALID CDa receberem certificados digitais emitidos pela AC VALID, e, cujos nomes aparecem no certificado digital, no campo "*Distinguished Name (DN)"*.

1.3.5. Aplicabilidade

Os certificados definidos por esta DPC AC VALID têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR).

1.4. DADOS DE CONTATO

Esta DPC é administrada pela Valid Certificadora Digital Ltda.

Endereço: Avenida Paulista, 1000 – São Paulo (SP)

CEP: 01310-100

Telefone: (11) 2575-6800

Página Web: http://www.validcertificadora.com.br

E-mail: acvalid@valid.com.br

1.4.1. Pessoas de Contato

Nome: Márcio Nunes da Silva

E-mail: marcio.nunes@valid.com.br

Telefone: (11) 2575-6800

2. DISPOSIÇÕES GERAIS

2.1. OBRIGAÇÕES E DIREITOS

2.1.1. Obrigações da AC VALID

As obrigações da AC VALID são as abaixo relacionadas:

a) operar de acordo com esta DPC;

b) gerar e gerenciar os seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

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 ACs de nível imediatamente subsequente 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 ACs de nível imediatamente subsequente ao seu;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

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

k) publicar a DPC AC VALID aprovada e implementada no endereço: http://icp-brasil.validcertificadora.com.br/ac-valid/dpc-ac-validv2.pdf

l) publicar em sua página web as informações definidas no item 2.6.1.2 deste documento;

m) não se aplica;

n) não se aplica;

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

p) adotar as medidas de segurança e controle previstas na DPC e Política de Segurança que implementar, 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 regularmente seu Plano de Continuidade do Negócio;

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

u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas condicionantes e limitações determinadas pela legislação vigente;

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

w) não emitir certificados com prazo de validade que se estenda além do prazo de validade de seu próprio certificado; e

x) fiscalizar suas ACs subsequentes, além da respectiva AR, habilitadas em conformidade com os critérios estabelecidos pelo Comitê Gestor (CG) da ICP-Brasil.

2.1.2. Obrigações da AR VALID CD

As obrigações da AR VALID CD são as abaixo relacionadas:

a) receber solicitações de cadastramento, de emissão e de revogação de certificados de AC de nível imediatamente subsequente ao seu;

b) confirmar a identidade do solicitante e a validade da solicitação;

c) não se aplica;

d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;

e) disponibilizar os certificados emitidos pela AC VALID aos seus respectivos solicitantes;

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

g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC VALID e pela ICP-Brasil;

h) manter e garantir a segurança da informação por ela 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 3.19, 3.1.10 e 3.1.11; e

k) garantir que todas as aprovações técnicas de solicitação de certificados sejam realizadas em instalações técnicas autorizadas.

l) acompanhar a geração do par de chaves e da solicitação do certificado da AC candidata a subsequente.

2.1.3. Obrigações do Titular do Certificado

As obrigações das ACs titulares de certificados emitidos de acordo com esta DPC AC VALID 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 nesta DPC e em outros documentos aplicáveis da AC VALID e da ICP-Brasil;

e) informar à AC VALID qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;

f) emitir certificados às ACs subsequentes, obedecendo aos padrões e requisitos constantes neste documento];

g) operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementar, estabelecidas em conformidade com os documentos REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [2], REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [3] e demais normas publicadas pela AC VALID e pela ICP-Brasil;

h) fornecer mensalmente relatórios de emissão de certificados à AC-Raiz.

2.1.4. Direitos da Terceira Parte (Relying Party)

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

2.1.4.2. Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos na PC ou DPC correspondente.

b) verificar a qualquer tempo a validade do certificado ICP-Brasil, sendo este considerado válido quando:

i. não constar da LCR da AC emitente;
ii. não estiver expirado; e
iii. puder ser verificado com o uso de certificado válido da AC emitente.

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

2.1.5. Obrigações do Repositório

O repositório da AC VALID é mantido em ambiente próprio e possui recursos físicos, humanos e de infraestrutura computacional aptos a:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC VALID 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 AC VALID

2.2.1.1. A AC VALID responderá pelos danos a que der causa.

2.2.1.2. A AC VALID responderá solidariamente pelos atos das entidades de sua cadeia de certificação, AC subordinadas, AR e eventuais PSS que venham a ser contratados.

2.2.2. Responsabilidades da AR

A AR VALID CD 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 (parte confiante) perante AC emitente de um certificado ou AR a ela vinculada, exceto na prática de ato ilícito.

2.3.2. Relações Fiduciárias

A AC VALID ou a AR VALID CD 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

Os processos administrativos cabíveis, relativos às operações da AC VALID e da AR vinculada, seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

2.4. INTERPRETAÇÃO E EXECUÇÃO

2.4.1. Legislação

A DPC AC VALID 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 e as Resoluções do CG da ICP-Brasil e as normas da AC VALID.

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 AC VALID examinará a disposição inválida e irá propor, 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 na DPC serão realizadas por iniciativa da AC VALID por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil e às AC subsequentes se for o caso.

2.4.3. Procedimentos de solução de disputa

2.4.3.1. Esta DPC prevalece sobre quaisquer outros documentos como planos, declarações, políticas, acordos e contratos que a AC VALID venha a adotar. Pode haver documentos complementares ou normativos, os quais não podem contrariar esta DPC. Em caso de conflito o documento conflitante deve ser ignorado ou alterado.

2.4.3.2. Em caso de 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 está DPC será alterada para a solução da disputa.

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

2.5. TARIFAS DE SERVIÇO

2.5.1. Tarifas de emissão e renovação de certificados

A AC VALID poderá definir custos para emissão ou renovação de certificados de AC de nível imediatamente subsequente ao seu. A emissão e renovação de certificados de AC de nível imediatamente ao seu poderá estar condicionada à celebração de acordos ou convênios.

2.5.2. Tarifas de acesso ao certificado

Não há tarifas previstas pela AC VALID para o acesso a seu certificado.

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

Não há tarifas previstas pela AC VALID para a revogação ou acesso a informações de *status* de certificados de AC de nível imediatamente subsequente ao seu.

2.5.4. Tarifas para outros serviços, tais como informação de política

Não há tarifas previstas pela AC VALID para outros serviços.

2.5.5. Política de reembolso

A AC VALID não estabelece política de reembolso.

2.6. PUBLICAÇÃO E REPOSITÓRIO

2.6.1. Publicação de informação da AC VALID

2.6.1.1. A AC VALID publica e disponibiliza informações, tais como certificados, LCR, sua DPC, entre outras, em página *WEB*, com disponibilidade de 99,50% (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. São publicados na página web da AC VALID em: http://www.validcertificadora.com.br/ac-valid

a) os certificados da AC VALID;

b) suas LCRs;

c) esta DPC.

2.6.2. Frequência de publicação

2.6.2.1. Os certificados e a LCR são publicados imediatamente após sua primeira emissão pela AC VALID. As LCR são publicadas a cada 45 dias, no máximo, independentemente de haver alteração. Esta DPC AC VALID é publicada após aprovação pela AC Raiz da ICP-Brasil.

2.6.2.2. As informações mencionadas neste item e no 2.6.1 serão publicadas sempre que sofrerem alterações.

2.6.3. Controles de acesso

2.6.3.1. O controle de acesso às informações publicadas pela AC VALID obedece ao estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

2.6.3.2. Não há qualquer restrição ao acesso para consulta a esta DPC, aos certificados emitidos e às LCRs da AC VALID.

2.6.3.3. Acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis, designadas especificamente para esse fim. Os controles de acesso incluirão identificação pessoal para acesso aos equipamentos, utilização de senhas e utilização de protocolos seguros de comunicação de dados.

2.6.4. Repositórios

O repositório da AC VALID está disponível 24 horas por 7 dias por semana para consulta e atende aos seguintes requisitos:

a) endereço: http://www.validcertificadora.com.br/ac-valid

b) disponibilidade: aquela definida no item 2.6.1 desta DPC AC VALID;

c) protocolo de acesso: HTTP;

d) características de segurança: aquelas definidas no item 5 desta DPC AC VALID.

Somente a AC VALID, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas em seu repositório.

2.6.4.1 A AC VALID disponibiliza um repositório para distribuição de LCR, no endereço: http://icp-brasil.validcertificadora.com.br/ac-valid/lcr-ac-validv5.crl

2.7. FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE

2.7.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades

integrantes da ICP-Brasil estão em conformidade com suas respectivas DPC, 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, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

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

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

2.7.5. As entidades da ICP-Brasil diretamente vinculadas à AC VALID – ACs e ARs também receberam auditoria prévia, para fins de credenciamento. A AC VALID 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. As chaves privadas de assinatura digital da AC VALID são geradas e mantidas pela própria AC VALID, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC VALID é de sua inteira responsabilidade.

2.8.1.2. Os titulares de certificados emitidos pela AC VALID, 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 dessas chaves.

2.8.1.3. Não se aplica.

2.8.2. Tipos de informações sigilosas

2.8.2.1. Todas as informações coletadas, geradas, transmitidas e mantidas pela AC VALID e a AR VALID CD são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3. Essas informações serão arquivadas de acordo com sua classificação, especificada na Política de Segurança.

2.8.2.2. Como princípio geral, nenhum documento, informação ou registro fornecido à AC VALID ou AR VALID CD deverá ser divulgado.

2.8.3. Tipos de informações não sigilosas

São consideradas informações não sigilosas:

a) os certificados e as LCRs emitidos pela AC VALID;

b) informações corporativas ou pessoais que necessariamente façam parte dos certificados ou de diretórios públicos;

c) não se aplica;

d) a DPC da AC VALID;

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 AC VALID disponibiliza a lista de certificados revogados em seu repositório, onde os motivos que justificaram a revogação são mantidos confidenciais pela AC VALID e pela AR VALID, exceto quando:

a) o titular do certificado revogado autorizar expressamente a sua divulgação a terceiros;

b) esses motivos tenham sido publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da AC VALID ou da AR VALID;

c) tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC VALID ou a AR VALID, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

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

2.8.5. Quebra de sigilo por motivos legais

A AC VALID tem o dever de fornecer documentos, informações ou registro sob sua guarda, mediante ordem judicial.

2.8.6. Informações a terceiros

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

2.8.7. Divulgação por solicitação do titular

2.8.7.1. O titular de certificado 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. Nenhuma liberação de informação é permitida sem autorização formal do titular do certificado, exceto nos casos do item 2.8.5. Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou

b) por meio de pedido escrito com firma reconhecida.

2.8.8. Outras circunstâncias de divulgação de informação

Em nenhuma outra circunstância, que não esteja prevista nesta DPC, serão divulgadas informações sigilosas.

2.9. DIREITOS DE PROPRIEDADE INTELECTUAL

Todos os direitos de propriedade intelectual inclusive os direitos autorais em todos os certificados e todos os documentos gerados para a AC VALID (eletrônicos ou não), pertencem e continuarão sendo de propriedade da AC VALID. Direitos sobre Identificadores de Objeto (OID) atribuídos à AC VALID após o processo de credenciamento cabem única e exclusivamente à AC Raiz da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. REGISTRO INICIAL

3.1.1. Disposições Gerais

3.1.1.1. A AR VALID, vinculada à AC VALID, utilizará os seguintes requisitos e procedimentos para a realização dos procedimentos que seguem:

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

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

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

b) não se aplica;

3.1.1.2. não se aplica;

3.1.1.3. não se aplica;

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 poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

3.1.1.5. Nos casos de certificado digital emitido para Servidores do Serviço Exterior Brasileiro, em missão permanente no exterior, assim caracterizados conforme a Lei nº 11.440, de 29 de dezembro de 2006, se houver impedimentos para a identificação conforme o disposto no subitem 3.1.1.1 deste anexo, é facultada a remessa da documentação pela mala diplomática e a realização da identificação por outros meios seguros, a serem definidos e aprovados pela AC-Raiz da ICP-Brasil.

3.1.1.6. Não se aplica.

3.1.1.7. Não se aplica.

3.1.1.8. Não se aplica.

3.1.2. Tipos de nomes

3.1.2.1. As ACs de nível imediatamente subsequente ao da AC VALID, titulares de certificados, terão um nome que as identifique univocamente no âmbito da ICP-Brasil.

a) o DN (*Distinguished Name*) dos certificados deverá seguir o padrão definido no item 7.1.4.

3.1.2.2. Certificados emitidos para ACs subsequentes não incluirão o nome da pessoa responsável.

3.1.3. Necessidade de nomes significativos

Para identificação dos titulares dos certificados emitidos, a AC VALID 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

Não se aplica.

3.1.5. Unicidade de nomes

Os identificadores "*Distinguished Name"* (DN) são únicos para cada AC de nível imediatamente subsequente ao da AC VALID. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509.

A extensão "*Unique Identifiers*" não será admitida para diferenciar as ACs com nomes idênticos.

3.1.6. Procedimento para resolver disputa de nomes

A AC VALID reserva-se o direito de tomar todas as decisões referentes a disputas de nomes das ACs de nível imediatamente subsequente 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

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

3.1.8. Método para comprovar a posse de chave privada

3.1.8.1. A AC VALID, por meio dos seus agentes de registro, acompanhará, no ambiente da AC candidata a subsequente, a geração do par de chaves e da solicitação do certificado (Certificate Request PKCS#07) contendo a chave

pública correspondente à chave privada gerada. A solicitação é gravada em mídia, que é verificada e guardada em envelope lacrado.

3.1.8.2. O envelope é então levado ao ambiente *offline* da AC VALID, onde é verificado quanto à violação e aberto na presença de representantes da AC VALID, da AC candidata e de testemunhas da AC VALID. A mídia é verificada novamente e é então utilizada no processo de emissão do certificado à AC subsequente.

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 pessoais de identificação legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

3.1.9.1.1. Deverá ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de indivíduo solicitante de certificado:

a) Cédula de Identidade ou Passaporte, se brasileiro;

b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;

c) Passaporte, se estrangeiro não domiciliado no Brasil;

d) comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial;

e) mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4;

f) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11]; e

g) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].

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

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. Não se aplica.

3.1.10. Autenticação da Identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.1.1. A confirmação da identidade de uma AC subordinada é feita com base no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL (DOC-ICP-03),

3.1.10.1.2. Será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

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

a) apresentação do rol de documentos elencado 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 certificado;

c) presença física do responsável pelo uso do certificado e assinatura do termo de responsabilidade de que trata o item 4.1.1; e

d) presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade de que trata o item 4.1.1.

3.1.10.2. Documentos para efeitos de identificação de uma organização

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

a) relativos a sua habilitação jurídica:

i. se pessoa jurídica cuja criação se deu ou foi autorizada 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 à sua habilitação fiscal:

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

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

3.1.10.3. Informações contidas no certificado emitido para uma organização:

3.1.10.3.1 Não se aplica.

3.1.10.3.2. Não se aplica.

3.1.11. Autenticação da identidade de equipamento ou aplicação

Não se aplica.

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

Não se aplica

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

Pode ser solicitado um novo certificado antes da expiração do atual, observando os mesmos requisitos e procedimentos exigidos para a solicitação de certificados.

3.2.1. O processo de geração, pela AC VALID, de um novo certificado para uma AC de nível imediatamente subsequente ao seu pode ser feito de forma simplificada, antes da expiração da validade do certificado vigente da AC.

3.2.2. Para isto, um representante legal da AC deve entregar assinado, em papel ou digitalmente, requisição de REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO. Após o recebimento dessa requisição, desde que a documentação esteja regularmente atualizada, a AC VALID iniciará o processo de emissão do novo certificado.

3.2.3. Não se aplica

3.3. CRIAÇÃO DE NOVO PAR DE CHAVES APÓS A EXPIRAÇÃO OU REVOGAÇÃO

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

3.3.2. Após a expiração ou revogação de certificado de AC de nível imediatamente subsequente ao da AC VALID, a AC Subsequente executa os processos regulares de geração de seu novo par de chaves.

3.4. SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado de AC de nível imediatamente subsequente será feita formalmente por representante legal da AC, que deve apresentá-la pessoalmente. A solicitação de revogação poderá ainda ser feita por decisão judicial, ou determinação da AC-Raiz.

4. REQUISITOS OPERACIONAIS

4.1. SOLICITAÇÃO DE CERTIFICADO

4.1.1. A solicitação de emissão de um Certificado Digital para Autoridade Certificadora imediatamente subsequente à AC VALID deverá ser feita por meio de documento formal do representante legal da AC candidata. Os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado são:

a) a comprovação de atributos de identificação constantes do certificado;

b) não se aplica;

c) um termo de titularidade assinado e um termo de responsabilidade assinado pelo representante legal da AC candidata, estabelecendo as condições de uso deste, elaborados conforme o documento MODELO DE TERMO DE TITULARIDADE [4].

4.1.2. A solicitação de certificado para AC de nível imediatamente subsequente ao da AC VALID somente é possível após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.3. Não se aplica.

4.1.4. A AC subsequente deverá encaminhar a solicitação de seu certificado à AC VALID por meio de seus representantes legais, utilizando 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 AC VALID é feita em cerimônia específica, com a presença de representantes da AC VALID, da AC habilitada, convidados e testemunhas, na qual são registrados todos os procedimentos executados.

4.2.2. A AC VALID garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 10 (dez) dias úteis após o recebimento da solicitação citada no item 4.1.3

4.2.3. A emissão dos certificados das ACs de nível imediatamente subsequente à AC VALID é feita em equipamentos que operam *offline*.

4.2.4. A AC VALID entrega o certificado emitido, no padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], para os representantes legais da AC habilitada.

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

4.3. ACEITAÇÃO DE CERTIFICADO

4.3.1. A AC VALID garante que as informações contidas no certificado emitido para uma AC de nível imediatamente subsequente ao seu foram verificadas de correspondente acordo com esta DPC.

4.3.2. A AC atestará por meio de seus representantes legais, mediante assinatura do “Termo de Acordo”, o recebimento do certificado emitido.

4.3.3. A aceitação do certificado se dá após a verificação pela AC ou na primeira utilização da chave privada. A AC titular tem o prazo de 2 (dois) dias úteis, contados do seu recebimento, para fazer a verificação dos dados do certificado. Após esse prazo o certificado é considerado aceito

4.3.4. Ao aceitar o certificado, a AC titular:

a) concorda com as responsabilidades, obrigações e deveres a ela impostos pelo Termo de Acordo e está DPC;

b) garante que com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

c) afirma que todas as informações de certificado fornecidas durante o processo de credenciamento são verdadeiras e estão reproduzidas no certificado de forma correta e completa;

d) aceita as regras e normas da AC VALID para emissão de certificados na sua cadeia de certificação.

4.3.5. A não aceitação do certificado dentro do prazo previsto implica a realização de nova cerimônia, onde é feita a revogação do certificado não aceito e a emissão de novo certificado.

4.4. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1. Circunstâncias para revogação

4.4.1.1. Um certificado de AC de nível imediatamente subsequente ao da AC VALID pode ser revogado a qualquer momento por solicitação da AC titular do certificado ou por decisão motivada da AC VALID ou da AC Raiz.

4.4.1.2. Um certificado é obrigatoriamente revogado:

a) quando constatada emissão imprópria ou defeituosa;

b) quando for necessária a alteração de qualquer informação nele constante;

c) no caso de dissolução da AC titular do certificado;

d) no caso de comprometimento da chave privada da AC ou da sua mídia armazenadora; ou

e) por decisão judicial.

4.4.1.3. Observa-se ainda que:

a) a AC VALID deverá revogar, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela AC VALID ou pela ICP-Brasil;

b) o CG da ICP-Brasil ou a AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.4.2. Quem pode solicitar revogação

A revogação do certificado de uma AC de nível imediatamente subsequente ao da AC VALID somente poderá ser solicitada:

a) pela AC VALID;

b) pela AR VALID CD;

c) pela AC titular do certificado;

d) pelo CG da ICP-Brasil;

e) pela AC Raiz;

f) por decisão judicial.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. A solicitação de revogação de certificado de AC subsequente deve ser feita por meio de do formulário SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC. Esse formulário deverá ser assinado pelo representante legal da AC. Se utilizada versão digital do documento, este deverá estar assinado digitalmente. O documento deverá ser entregue pessoalmente na AR VALID CD pelo representante legal da AC subsequente, e, em se tratando de formulário em papel, será assinado no ato da entrega.

4.4.3.2. Como diretrizes gerais, fica estabelecido que:

a) o solicitante da revogação de um certificado será 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 serão 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, e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado na base de dados da AC.

4.4.3.3. Não se aplica.

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

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

4.4.3.6. Não se aplica.

4.4.4. Prazo para solicitação de revogação

4.4.4.1. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1. O prazo para aceitação do certificado pelo titular é de 2 (dois) dias úteis, dentro desse prazo a revogação do certificado pode ser solicitada sem ônus.

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 AC VALID.

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 AC VALID.

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 AC VALID.

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 AC VALID.

4.4.9. Frequência de emissão de LCR

4.4.9.1. Neste item é definida a frequência para a emissão de LCR da AC VALID.

4.4.9.2. Não se aplica.

4.4.9.3. A frequência máxima para emissão de LCR é de 45 dias. Em caso de revogação de certificado emitido pela AC VALID, será emitida nova LCR no prazo previsto no item 4.4.3 e notificadas todas as ACs de nível imediatamente subsequente ao seu e a AC-Raiz.

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 deverá também ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

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

A AC VALID não disponibiliza recursos para revogação *on-line* de certificados.

4.4.12. Requisitos para verificação de revogação on-line

Não se aplica.

4.4.13. Outras formas disponíveis para divulgação de revogação

Além das LCRs, a AC VALID poderá utilizar outros meios para divulgação de informações de revogação de certificados de AC de nível imediatamente subsequente ao seu, incluindo publicação na sua página web.

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

As formas de verificação descritas no item anterior são meramente informativas.

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 subsequente ao da AC VALID, essa notificará imediatamente à AC VALID.

4.4.15.2. A comunicação do comprometimento da chave privada de uma AC poderá ser feita por correio eletrônico assinado digitalmente pelo representante legal da AC.

4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1. Tipos de Evento Registrados

4.5.1.1. A AC VALID 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 AC VALID;

c) mudanças na configuração da AC VALID ou nas suas chaves;

d) mudanças nas políticas de criação de certificados;

e) tentativas de acesso (*login*) e de saída do sistema (*logoff*);

f) tentativas não autorizadas de acesso aos arquivos de sistema;

g) geração de chaves próprias da AC VALID 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 AC VALID 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 meios 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 AC VALID 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. Todo o registro de auditoria, eletrônico ou manual, 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 AC VALID é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil [8].

4.5.1.6. Não se aplica.

4.5.1.7. Não se aplica.

4.5.2. Frequência de auditoria de registros (*logs*)

4.5.2.1. A análise dos registros de auditoria será realizada sempre que houver utilização de seu sistema de certificação (o equipamento é *offline,* permanecendo desligado a maior parte do tempo) ou em caso de suspeita de comprometimento da segurança.

4.5.2.2. Os registros de auditoria são analisados pela Área de Segurança da AC VALID. 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 AC VALID mantém localmente, nas suas instalações, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4. Proteção de registro (log) de Auditoria

4.5.4.1. Os equipamentos da AC VALID, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança.

4.5.4.2. A inspeção contínua dos diversos registros dos sistemas é feita por meio das ferramentas nativas do sistema operacional, do banco de dados e do aplicativo de AC, e estão disponíveis somente para leitura. Pode ser feita também por relatórios emitidos a partir destas ferramentas. Esses dados de auditoria são coletados e armazenados toda a vez que existir utilização do equipamento, em uma sala de arquivos de nível 3 de segurança.

4.5.4.3. Os registros de auditoria gerados eletrônica ou manualmente 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.

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

A AC VALID executa procedimentos de *backup* de todo o sistema de certificação, sempre que houver utilização, 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 AC VALID é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC VALID, pelo sistema de controle de acesso e pelo pessoal operacional.

TIPO DE EVENTO	*SISTEMA DE COLEÇÃO*	*REGISTRADO POR*
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de *log-in* e *log-out*	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional

Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados	Automático	AC ou *Software* de AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado	Automático	*Software* de AR
Logs de *Backup* e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de *software* e *hardware*	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	*Software* de controle de acesso e pessoal de operações

4.5.7. Notificação de agentes causadores de eventos

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

4.5.8. Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a AC VALID. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação. Eventos que indiquem possível vulnerabilidade, detectados na análise dos registros de auditoria da AC VALID, são analisados detalhadamente e, dependendo de sua gravidade, registrados

em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

4.6. A RQUIVAMENTO DE REGISTROS

4.6.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC VALID:

a) solicitações de certificados;

b) solicitações de revogação de certificados;

c) notificações de comprometimento de chaves privadas;

d) emissões e revogações de certificados;

e) emissões de LCR;

f) trocas de chaves criptográficas da AC VALID;

g) informações de auditoria previstas no item 4.5.1;

h) correspondências formais;

i) processos de credenciamento de AC de nível imediatamente subsequente ao da AC VALID.

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 são retidos permanentemente, para fins de consulta histórica;

b) as cópias dos documentos de identificação apresentados no momento da solicitação e da revogação de certificados e os termos de titularidade e responsabilidade serão retidos, no mínimo, por 10 anos a contar da data de expiração ou revogação do certificado; e

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

4.6.3. Proteção de arquivos

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da ICP-Brasil. Mídias de arquivos são guardadas em local seguro, sendo que a proteção criptográfica das mídias é adotada quando a

classificação da informação assim o exigir. Também são protegidas de fatores ambientais como temperatura, umidade e magnetismo.

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 AC VALID, protegido com o mesmo tipo de proteção utilizada no arquivo principal.

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

4.6.4.3 A AC VALID garante que a verificação da integridade dessas cópias de segurança, é realizada no mínimo, a cada 6 (seis) meses.

4.6.5. Requisitos para datação (*time-stamping*) de registros

Os servidores da AC VALID 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 AC VALID 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*	*REGISTRO POR*
Solicitações de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados	Automático	*Software* de AC/AR
Emissões de LCR	Automático	*Software* de AC/AR
Correspondências formais	Manual	Pessoal de

		operações

4.6.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC VALID, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado. Não serão disponibilizadas informações sigilosas para verificação.

4.7. TROCA DE CHAVE

4.7.1. A AC de nível imediatamente subsequente ao da AC VALID deverá iniciar, até 90 dias antes da expiração do seu certificado, o processo de geração de novo par de chaves e de emissão de novo certificado.

4.7.2. Uma vez expirado o certificado de uma AC de nível imediatamente subsequente ao seu, a AC VALID remove imediatamente esse certificado do diretório e de sua página WEB, mas o mantém armazenado em suas bases de dados permanentemente para efeito de consulta histórica.

4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

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

4.8.1. Recursos computacionais, *software* ou dados corrompidos

A AC VALID possui um PCN, de caráter sigiloso, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. O PCN 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 AC VALID.

4.8.2. Certificado de entidade revogado

A AC VALID possui um Plano de Continuidade de Negócio – PCN de caráter sigiloso, que especifica as ações a serem tomadas no caso em que o certificado da AC VALID for revogado, as quais se resumem no seguinte:

a) em caso de revogação do certificado da AC VALID, 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.

b) a seguir são revogados os certificados das ACs de nível imediatamente subsequente. É gerado novo par de chaves da AC VALID, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado. A AC VALID emite então novos certificados digitais para as ACs de nível imediatamente subsequente.

4.8.3. Chave de entidade comprometida

A AC VALID possui um PCN que especifica as ações a serem tomadas no caso em que a chave privada da AC VALID for comprometida, e que se resumem no seguinte:

a) em caso de comprometimento da chave da AC VALID, 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.

b) na confirmação do incidente, são revogados os certificados da AC VALID e das ACs de nível imediatamente subsequente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado. A seguir são emitidos, pela AC VALID, novos certificados digitais para as ACs de nível imediatamente subsequente, observados os procedimentos regulamentares.

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

4.8.4.1.A AC VALID possui um PCN 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 AC VALID quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

4.8.4.2. O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC VALID faz parte. Isto significa que o plano deve ter como meta primária restabelecer a AC VALID para tornar acessíveis 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

A AR VALID, por ser interna à AC VALID, utiliza o PCN da própria AC VALID onde são descritos os procedimentos previstos para recuperação total ou parcial das atividades da AC VALID, entre os quais:

a) identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios;

b) identificação e concordância de todas as responsabilidades e procedimentos definidos;

c) implementação dos procedimentos de emergência que permitam recuperação e restauração nos prazos necessários;

d) documentação dos processos e procedimentos acordados;

e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;

f) teste e atualização dos planos.

4.9. EXTINÇÃO DOS SERVIÇOS DE AC VALID OU DA AR VALID CD

4.9.1. A AC VALID 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 AC VALID ou da AR VALID, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes, inclusive:

a) notificar a AC Raiz da ICP-Brasil;

b) notificar todas as entidades subordinadas;

c) providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;

d) transferir progressivamente o serviço e os registros operacionais para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC VALID e AR VALID;

e) preservar qualquer registro não transferido a um sucessor;

f) transferir, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e

g) repassar à AC Raiz os documentos referentes aos certificados digitais e as respectivas chaves públicas, caso essas não sejam assumidas por outra AC.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAS

5.1. CONTROLE FÍSICO

5.1.1. Construção e localização das instalações

5.1.1.1. A operação da AC VALID é executada dentro de um ambiente físico seguro em área de instalação altamente protegida. A localização e o sistema de certificação utilizado para a operação da AC VALID 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. Nenhuma das linhas telefônicas dentro do ambiente de certificação da AC oferece suporte a modem.

5.1.1.2. Todas as instalações da AC VALID, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos a seguir:

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, estabilizadores e similares;

b) instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas;

c) iluminação de emergência.

5.1.2. Acesso físico

O acesso físico às dependências da AC VALID é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso. O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes. O sistema de certificação da AC VALID está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.2.1 Níveis de Acesso

5.1.2.1.1. São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC VALID, 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 AC VALID. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armado. A partir desse

nível, pessoas estranhas à operação da AC VALID transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC VALID é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido no ambiente onde estão instalados os equipamentos utilizados na operação da AC VALID, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, vídeo, som ou similares, bem como computadores portáteis, têm 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. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas por meio eletrônico e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC VALID.

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 AC VALID. 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 estejam envolvidas com essas atividades 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 AC VALID, 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 AC VALID, 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 ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que

constituem 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. A AC VALID possui um único ambiente para abrigar os equipamentos de produção *online*, os equipamentos de produção *off-line,* o cofre de armazenamento e os equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

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

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

a) ser feito em aço ou material de resistência equivalente;

b) possuir tranca com chave.

5.1.2.1.14. **O sexto nível – ou nível 6** - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da AC VALID 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 mídias de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da mídia) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma mídia referente a cada semana. Essas mídias 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. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.

5.1.2.2.4. Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, 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, é permanentemente monitorado 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 AC VALID 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

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

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

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

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

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

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

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

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

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

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

a) geradores de porte compatível;

b) geradores de reserva;

c) sistemas de "*no-breaks"* redundantes;

d) sistemas redundantes de ar condicionado.

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio

5.1.5.1. Todas as instalações da AC VALID possuem sistemas de prevenção contra incêndio. 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 sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2. Nas instalações da AC VALID 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 AC VALID, a temperatura interna da sala cofre não excede 50 graus Celsius e a sala suporta essa condição por, no mínimo, uma hora.

5.1.6. Armazenamento de mídia

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

5.1.7. Destruição de lixo

5.1.7.1. Todos os documentados 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)

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

5.1.9. Instalações Técnicas de AR

Não se aplica.

5.2. CONTROLES PROCEDIMENTAIS

5.2.1. Perfis qualificados

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC VALID, 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.

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

5.2.1.2. A AC VALID estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as ações 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 AC VALID 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 AC VALID, conforme o descrito em 6.2.2.

5.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC VALID necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC VALID. As demais tarefas da AC poderão ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

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

a) ser incluído em uma lista de acesso às instalações da AC VALID;

b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC VALID;

c) receber um certificado para executar suas atividades operacionais na AC VALID;

d) receber uma conta no sistema de certificação da AC VALID.

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 AC VALID devidamente qualificado);

b) não são compartilhados;

c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC VALID implementa um padrão de utilização de "senhas fortes", definido em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

5.3. CONTROLES DE PESSOAL

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC VALID e pela AR VALID CD em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os empregados da AC VALID e da AR VALID, 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 AC VALID;

c) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;

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 AC VALID 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 AC VALID 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 AC VALID, 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;

d) comprovação de escolaridade e de residência.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC VALID e da AR vinculada, 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 AC VALID e da AR vinculada;

b) sistema de certificação em uso na AC VALID;

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. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC VALID e da AR vinculada 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 AC VALID e no sistema das ARs.

5.3.5. Frequência e sequência de rodízios de cargos

A AC VALID não implementa rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC VALID suspenderá o seu acesso ao sistema de certificação e tomará as medidas administrativas e legais cabíveis.

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

a) relato da ocorrência com "*modus operandi*";

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 AC VALID 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 AC VALID e da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC VALID, da AR Vinculada e das ACs de nível imediatamente subsequente, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, será contratado conforme o estabelecido nas Política de Segurança da ICP-Brasil[8] e na Política de Segurança da AC VALID.

5.3.8. Documentação disponibilizada ao pessoal

5.3.8.1. A AC VALID disponibiliza para todo o seu pessoal, para as ACs de nível imediatamente subsequente ao seu e para a AR vinculada:

a) está DPC;

b) não se aplica;

c) a Política de Segurança da ICP-Brasil;

d) documentação operacional relativa às suas atividades;

e) contratos, normas e políticas relevantes para suas atividades; e

f) a Política de Segurança da AC VALID.

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 criptográficas da AC VALID é gerado pela própria AC VALID, após ter sido credenciada e autorizada a funcionar no âmbito da ICP-Brasil.

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

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

O par de chaves da AC VALID é gerado em módulos criptográficos de hardware, conforme definido no DOC-ICP-01.01, com padrão de segurança FIPS 140- 2 nível 3 (para a cadeia de certificação V2) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5) definido no DOC-ICP-01.

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

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

O par de chaves das AC Subsequente é gerado e armazenado em módulo criptográfico de hardware, conforme definido no DOC-ICP-01.01, com padrão de segurança FIPS 140-2 nível 3 (para cadeia de certificação V2) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5) definido no DOC-ICP-01.

6.1.1.3. Não se aplica.

6.1.2. Entrega da chave privada à entidade titular

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

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC VALID 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 AC VALID, 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 acordada entre as partes.

6.1.4. Disponibilização de chave pública da AC VALID para usuários

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

a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];

b) na página *web:* http://www.validcertificadora.com.br/ac-valid

c) 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 mínimo das chaves criptográficas associadas aos certificados da AC VALID é de RSA 4096 bits (V2 e V5), conforme definido no DOC-ICP-01.01.

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC VALID adotam o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas referenciadas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8. Geração de chave por *hardware* ou *software*

6.1.8.1. A AC VALID utiliza componentes seguros de *hardware* para a geração de seus pares de chaves, de seus certificados, dos certificados das ACs de nível imediatamente subsequente ao seu e para a geração de suas LCR. Os componentes seguros de *hardware* utilizam mecanismos de prevenção e detecção de violação.

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. As chaves criptográficas dos titulares de certificados emitidos pela AC VALID (ACs subsequentes) poderão ser utilizadas apenas para assinatura dos certificados por elas emitidos e de suas LCRs.

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

6.2. PROTEÇÃO DA CHAVE PRIVADA

As chaves privadas da AC VALID são armazenadas de forma cifrada nos mesmos componentes seguros de *hardware* utilizados para sua geração. O acesso a esses componentes é controlado por meio de chave criptográfica de ativação.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC VALID adota o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Os módulos criptográficos das ACs subsequentes à AC VALID devem adotar padrões definidos 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 AC VALID é dividida em 8 (oito) partes e distribuídas por 8 (oito) custodiantes designados pela AC VALID (m).

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

6.2.3. Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas das ACs de nível imediatamente subsequente. 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 AC VALID 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 AC VALID não mantém cópia de segurança das chaves privadas das ACs de nível imediatamente subsequentes 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].

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas dos titulares de certificados emitidos pela AC VALID 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 AC VALID é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7. Método de ativação de chave privada

A ativação das chaves privadas da AC VALID é implementada por meio do módulo criptográfico, após identificação dos operadores responsáveis. Esta identificação é realizada por meio de senha e de tokens ou cartões criptográficos, após a identificação de 2 (dois) dos 8 (oito) custodiantes da chave criptográfica de ativação. Os custodiantes da chave de ativação são funcionários indicados pelo representante legal da AC VALID.

6.2.8. Método de desativação de chave privada

A chave privada da AC VALID, armazenada em módulo criptográfico é desativada, quando não mais necessária, por meio 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 tokens ou cartões criptográficos, protegidos com senha, após a identificação de 2 (dois) dos 8 (oito) custodiantes da chave criptográfica de ativação.

6.2.9. Método de destruição de chave privada

Quando a chave privada da AC VALID for desativada, em decorrência de expiração ou revogação, ela 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 AC VALID 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 AC VALID.

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. Arquivamento de chave pública

As chaves públicas da própria AC VALID, e dos titulares dos certificados por ela emitidos, bem como as LCR emitidas, serão armazenados pela AC VALID, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. A chave privada da AC VALID bem como as chaves privadas dos titulares dos certificados por ela emitidos deverão ser utilizadas apenas durante o período de validade do certificado correspondente. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. . Não se aplica

6.3.2.4. Os certificados emitidos pela AC VALID para as ACs de nível imediatamente subsequente ao seu terão validade de no máximo 8 (oito) anos.

6.4. DADOS DE ATIVAÇÃO

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação da chave privada da AC VALID são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em *hardware (token* ou cartão criptográfico*)*.

6.4.1.2. Não se aplica.

6.4.2. Proteção dos dados de ativação.

6.4.2.1. Os dados de ativação das chaves privadas da AC VALID são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Não se aplica.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A AC VALID garante que a geração de seu par de chaves é realizada em ambiente *offline,* 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 ACs titulares de certificados emitidos pela AC VALID devem ser os mesmos descritos no item abaixo para os computadores servidores da AC VALID.

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

a) controle de acesso aos serviços e perfis da AC VALID;

b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC VALID;

c) acesso restrito aos bancos de dados da AC VALID;

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 AC VALID;

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 da AC VALID 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 AC VALID ou AC subsequente. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC VALID ou às AC subsequentes 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 AC VALID aplica configurações de segurança definidas como EAL3, baseadas no Common Criteria e desenvolvidas para o sistema operacional Red Hat Enterprise Linux. O fabricante disponibiliza as atualizações do sistema operacional utilizado nos servidores do Sistema de Certificação Digital da AC VALID.

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 AC VALID adota sistema de certificação desenvolvido em código aberto; todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após a conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente de Operações da AC VALID avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2. Controle de gerenciamento de segurança

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

a) a AC VALID opera em equipamento *offline*, portanto não necessita configuração de segurança de rede;

b) 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.

6.6.2.2. O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC VALID, envolve testes 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 de certificados, páginas *web*, *scripts* etc.;

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

d) instalação de novos serviços na plataforma de processamento.

6.6.3. Classificação de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

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

6.7. CONTROLES DE SEGURANÇA DE REDE

6.7.1. Diretrizes Gerais

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

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

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

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

6.7.1.5. O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de

dados, que permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2. Firewall

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

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

6.7.3. Sistema de detecção de intrusão (IDS)

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

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

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

6.7.4. Registro de acessos não autorizados à rede

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

6.8. CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

O módulo criptográfico utilizado para armazenamento da chave privada da AC VALID está em conformidade com o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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 AC VALID.

7.1.2. Não se aplica.

7.1.3. Nos itens seguintes está especificado o formato dos certificados emitidos pela AC VALID.

7.2. PERFIL DO CERTIFICADO

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

7.2.1. Número(s) de versão

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

7.2.2. Extensões de certificados

Os certificados emitidos pela AC VALID, sob esta DPC, obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

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

b) **"*Subject Key Identifier*", não crítica**: contém o *hash* da chave pública da AC titular do certificado;

c) "***Key Usage*", crítica**: somente os bits e *keyCertSign* e *cRLSign* são ativados;

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

d.1) o campo ***policyIdentifie***r contém o OID das PC que a AC titular do certificado implementa;

d.2) o campo ***policyQualifiers*** contém o endereço *URL* da página *web onde se obtém a DPC da AC VALID:* http://icp-brasil.validcertificadora.com.br/ac-valid/dpc-ac-validv2.pdf

e) "***Basic Constraints***", crítica, deve conter:

e.1) Subjec tType=CA e;

e.2) Path Lenght Constraint=0 (zero)

f) "***CRL Distribution Points*", não crítica**: contém os endereços *URL* das duas páginas *web* onde se obtém a LCR da AC VALID:

Para Certificados da cadeia V2:

f.1 http://icp-brasil.validcertificadora.com.br/ac-valid/lcr-ac-validv2.crl

f.2 http://icp-brasil2.validcertificadora.com.br/ac-valid/lcr-ac-validv2.crl

f.3 http://repositorio.icpbrasil.gov.br/lcr/valid/lcr-ac-validv2.crl

Para Certificados da cadeia V5:

f.1 http://icp-brasil.validcertificadora.com.br/ac-valid/lcr-ac-validv5.crl

g) "***Authority Information Access*",** não crítica, contendo o endereço na Web onde se obtém o arquivo p7b com os certificados da cadeia:

Para Certificados da cadeia V2:
http://icp-brasil.validcertificadora.com.br/ac-valid/ac-validv2.p7b

Para Certificados da cadeia V5:
http://icp-brasil.validcertificadora.com.br/ac-valid/ac-validv5.p7b

7.2.3. Identificadores de algoritmos

Os certificados emitidos pela AC VALID são assinados com o uso do algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

7.2.4. Formatos de nome

Para os certificados emitidos sob a DPC AC VALID, 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= Razão Social da AC subsequente

CN= Nome da AC subsequente

O CN deverá estar na forma "AC < nome da AC titular>

No formato os caracteres “<’ e “>” delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

7.2.5. Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC VALID 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 AC VALID após conclusão do processo de seu credenciamento, é **2.16.76.1.1.43**.

7.2.7. Uso da extensão "Policy Constraints"

A extensão "*Policy Constraints*" poderá ser utilizada, da forma definida na RFC 5280, em certificados emitidos pela AC VALID.

7.2.8. Sintaxe e semântica dos qualificadores de política

O campo *policyQualifiers* da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC VALID.

7.2.9. Semântica de processamento para extensões criticas

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

7.3. Perfil de LCR

7.3.1. Número (s) de versão

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

7.3.2. Extensões de LCR e de suas entradas

7.3.2.1. A AC VALID adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) "***Authority Key Identifier***": contém o hash SHA-1 da chave pública da AC VALID que assina a LCR.

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

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração nesta DPC da AC VALID será submetida previamente à aprovação do CG da ICP-Brasil.

8.2. POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO

A AC VALID publica e mantém atualizada está DPC, em seu repositório (item 2.4.6, alínea “a”)

8.3. PROCEDIMENTOS DE APROVAÇÃO

Esta DPC foi submetida à aprovação da AC-RAIZ da ICP-Brasil, durante o processo de credenciamento da AC VALID, conforme o determinado pelo documento “CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]”.

9. DOCUMENTOS REFERENCIADOS

9.1. Os documentos listados a seguir 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

[11]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05

9.2. Os documentos a seguir 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 ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	DOC-ICP-05.02
[11]	REGULAMENTO DO USO DE BIOMETRIA NO ÂMBITO DA ICP BRASIL – SISTEMA BIOMÉTRICO DA ICPBRASIL	DOC-ICP-05.03

9.3. Os documentos a seguir 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]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.B