Declaração de Práticas de Certificação

da Autoridade Certificadora

ONLINE BRASIL

(DPC da AC ONLINE BRASIL)

OID 2.16.76.1.1.61
Versão 1.1 de 20.07.2015

Sumário

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

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 ONLINE BRASIL, AC ONLINE BRASIL, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, na execução dos seus serviços.

1.1.2. A AC ONLINE BRASIL possui certificados de segundo nível na ICP-Brasil, assinados pela AC VALID. Os certificados da AC ONLINE BRASIL contêm as chaves públicas correspondentes às chaves privadas utilizadas para assinar os certificados de assinatura A1 e A3 e as suas LCRs (Listas de Certificados Revogados).

1.1.3. A AC ONLINE BRASIL utiliza ambiente de Prestador de Serviços de Suporte para hospedar, operar e dar manutenção às suas atividades.

1.1.4. A estrutura desta DPC AC ONLINE BRASIL 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.

1.1.5 Para regulamentar usos específicos dos certificados emitidos pela AC ONLINE BRASIL são publicadas Políticas de Certificados (PCs) disponíveis em página web http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/

1.2. IDENTIFICAÇÃO

Este documento é chamado “Declaração de Práticas de Certificação da Autoridade Certificadora ONLINE BRASIL” e comumente referido como “DPC AC ONLINE BRASIL”. O Identificador de Objeto **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.61.**

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. Autoridades Certificadoras

Esta DPC refere-se unicamente à Autoridade Certificadora ONLINE BRASIL (AC ONLINE BRASIL) e encontra-se publicada no seu repositório, no seguinte endereço: http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/

1.3.2. Autoridades de Registro

1.3.2.1 Os processos de identificação, cadastramento, recebimento de solicitações de renovação e revogação de certificados digitais e de identificação de seus solicitantes são de competência das Autoridades de Registro (ARs) vinculadas. A AC ONLINE BRASIL disponibiliza e mantém atualizada na página http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/ as seguintes informações referentes às ARs vinculadas:

a) relação de todas as ARs credenciadas, com informações sobre as PC que implementam;

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

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

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

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

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

1.3.2.2 A AC ONLINE BRASIL mantém as informações acima atualizadas.

1.3.3. Prestador de Serviços de Suporte

1.3.3.1 A AC ONLINE BRASIL utiliza os seguintes Prestadores de Serviço de Suporte (PSS) nas suas operações:

a) VALID CERTIFICADORA DIGITAL LTDA.

b) VALID SOLUÇÕES E SERVIÇOS DE SEGURANÇA EM MEIOS DE PAGAMENTO E IDENTIFICAÇÃO S.A.

Essa informação encontra-se na página web http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/

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

a) disponibilização de Infraestrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

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

1.3.3.3 A AC ONLINE BRASIL mantém as informações acima atualizadas.

1.3.4. Titulares de Certificado

1.3.4.1 Pessoas físicas ou jurídicas, de direito público ou privado, nacionais ou estrangeiras, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis, podem ser Titulares de Certificado. Os certificados podem ser utilizados por pessoas físicas, pessoas jurídicas, em equipamentos ou aplicações.

1.3.4.2. Em sendo o titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada.

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

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

1.3.5. Aplicabilidade

A AC ONLINE BRASIL implementa as seguintes políticas de certificado digital:

Política de Certificado	**Nome**	**OID**
Política de Certificado de Assinatura Digital do tipo A1 da AC ONLINE BRASIL	PC A1 da AC ONLINE BRASIL	2.16.76.1.2.1.48

Política de Certificado de Assinatura Digital do tipo A3 da AC ONLINE BRASIL	PC A3 da AC ONLINE BRASIL	2.16.76.1.2.3.45

1.4. DADOS DE CONTATO

Dados de Contato

Esta DPC é administrada pela ONLINE CERTIFICADORA LTDA - ME

Endereço: Av. Miguel Sutil, 8.388 – Salas 604, 605, 608 e 609 – Ed. Avantgarde Business – Santa Rosa – Cuiabá/MT.

CEP: 78040-365

Telefone: (65)2121-0886

Página Web: www.onlinecertificadora.com.br

E-mail: aconline@onlinecertificadora.com.br

Pessoas de Contato

Nome: Júlio Cesar Morais e Souza

E-mail: julio.souza@onlinecertificadora.com.br

Telefone: (65) 2121-0886

2. DISPOSIÇÕES GERAIS

2.1. OBRIGAÇÕES E DIREITOS

2.1.1. Obrigações da AC ONLINE BRASIL

As obrigações da AC ONLINE BRASIL 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 os seus usuários 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 de usuários finais;

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 ONLINE BRASIL aprovada e implementada no endereço: http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/dpc-ac-onlinebrasil.pdf

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

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

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

o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo 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;

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.

2.1.2. Obrigações das ARs vinculadas à AC ONLINE BRASIL

As obrigações ARs vinculadas são as abaixo relacionadas:

a) receber solicitações de cadastramento, de emissão e de revogação de certificados;

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

c) encaminhar a solicitação de emissão ou de revogação de certificado à AC responsável utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL[1];

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

e) disponibilizar os certificados emitidos pela AC ONLINE BRASIL 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 ONLINE BRASIL 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.

2.1.3. Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos de acordo com esta DPC AC ONLINE BRASIL 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 ONLINE BRASIL e da ICP-Brasil;

e) informar à AC ONLINE BRASIL qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

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

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

As obrigações da AC ONLINE BRASIL em relação ao seu repositório são:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC ONLINE BRASIL e a sua LCR;

b) manter o repositório 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 armazenados no repositório.

2.2. RESPONSABILIDADES

2.2.1. Responsabilidades da AC ONLINE BRASIL

2.2.1.1. A AC ONLINE BRASIL responderá pelos danos a que der causa.

2.2.1.2. A AC ONLINE BRASIL responderá solidariamente pelos atos das entidades de sua cadeia de certificação, AR e PSS contratados.

2.2.2. Responsabilidades da AR

As ou ARs vinculadas à AC ONLINE BRASIL serão responsáveis 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 ARs vinculadas, exceto na prática de ato ilícito.

2.3.2. Relações Fiduciárias

2.3.2.1. A AC ONLINE BRASIL dispõe de uma apólice de seguro de responsabilidade civil que se estende a todos os titulares de certificados digitais por ela emitidos.

2.3.2.2. A AC ONLINE BRASIL ou suas ARs vinculadas indenizarão integralmente os danos a que comprovadamente derem causa, limitados ao valor máximo coberto pela apólice, caso o cliente seja Pessoa Jurídica.

2.3.2.3. A apólice de seguro de responsabilidade civil cobre perdas e danos decorrentes de comprometimento da chave privada da AC ONLINE BRASIL, de erro na identificação do titular, de emissão defeituosa do certificado ou de erros ou omissões da AC ONLINE BRASIL e das ARs vinculadas na prestação de seus serviços.

2.3.3. Processos Administrativos

O titular do certificado que sofrer perdas e danos decorrentes do uso do certificado digital emitido pela AC ONLINE BRASIL tem o direito de comunicar à AC ONLINE BRASIL que deseja a indenização prevista no item 2.3.2 acima, observadas as seguintes condições:

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC ONLINE BRASIL, tal comprometimento deverá ter sido comprovado por perícia realizada por perito especializado e independente;

b) nos casos de erro na identificação, o titular do certificado não pode requerer qualquer indenização quando os dados constantes no certificado corresponderem aos dados fornecidos por esse titular à AC ONLINE BRASIL ou às ARs vinculadas;

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

2.4. INTERPRETAÇÃO E EXECUÇÃO

2.4.1. Legislação

A DPC AC ONLINE BRASIL 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 ONLINE BRASIL.

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 ONLINE BRASIL 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, relativas às práticas descritas na DPC, realizadas por iniciativa da AC ONLINE BRASIL, serão enviadas por e-mail assinado pelos responsáveis pela AC.

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 ONLINE BRASIL 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 às normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nessa situação esta 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 ONLINE BRASIL define tarifas para emissão ou renovação de certificados conforme estabelecido em sua página web www.onlinecertificadora.com.br ou em contrato comercial específico.

2.5.2. Tarifas de acesso ao certificado

Não há tarifas previstas pela AC ONLINE BRASIL 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 ONLINE BRASIL para a revogação. Pelo acesso a informação de status a tarifa é variável conforme definição interna da AC ONLINE BRASIL.

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

Não há tarifas previstas pela AC ONLINE BRASIL para outros serviços.

2.5.5. Política de reembolso

Caso o certificado deva ser revogado por motivo de comprometimento da chave privada da AC ONLINE BRASIL ou da mídia armazenadora da chave privada da AC ONLINE

BRASIL, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC ONLINE BRASIL, será emitido outro certificado em substituição, sem cobrança.

2.6. PUBLICAÇÃO E REPOSITÓRIO

2.6.1. Publicação de informação da AC ONLINE BRASIL

2.6.1.1. A AC ONLINE BRASIL publica e disponibiliza informações, tais como certificados, LCR, sua DPC, entre outras, 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 ONLINE BRASIL em http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/

a) os certificados da AC ONLINE BRASIL;

b) suas LCRs;

c) esta DPC;

d) as PCs que implementa;

e) uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;

f) uma relação, regularmente atualizada, das ARs vinculadas que tenham celebrado acordos operacionais com outras ARs da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e

g) uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2. Frequência de publicação

Certificados da AC ONLINE BRASIL são publicados imediatamente após sua emissão. A publicação das LCRs se dá conforme determinado na PC correspondente. As versões ou alterações desta DPC e das PCs, assim como os endereços das instalações técnicas das ARs vinculadas, são atualizados no web site da AC ONLINE BRASIL após aprovação da AC Raiz da ICP-Brasil.

2.6.3. Controles de acesso

2.6.3.1. Não há qualquer restrição ao acesso para consulta às informações citadas no item 2.6.1.

2.6.3.2. 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 ONLINE BRASIL está disponível para consulta e atende aos seguintes requisitos:

a) endereço: http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/

b) disponibilidade: aquela definida no item 2.6.1 desta DPC AC ONLINE BRASIL

c) protocolo de acesso: HTTP;

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

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 ONLINE BRASIL 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 ONLINE BRASIL também receberam auditoria prévia, para fins de credenciamento. A AC ONLINE BRASIL 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 ONLINE BRASIL são geradas e mantidas pela própria AC ONLINE BRASIL, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC ONLINE BRASIL é de sua inteira responsabilidade.

2.8.1.2. Os titulares de certificados emitidos pela AC ONLINE BRASIL 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 ONLINE BRASIL e pelas ARs vinculadas 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 ONLINE BRASIL ou às ARs vinculadas deverá ser divulgado.

2.8.3. Tipos de informações não sigilosas

2.8.3.1 São consideradas informações não sigilosas:

a) os certificados e as LCRs emitidos pela AC ONLINE BRASIL;

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

c) não se aplica;

d) a DPC da AC ONLINE BRASIL;

e) versões públicas de Políticas de Segurança; e

f) a conclusão dos relatórios de auditoria.

2.8.3.2 A AC ONLINE BRASIL e as ARs vinculadas tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

a) estejam na posse legítima da AC ONLINE BRASIL e das ARs vinculadas antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;

b) posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação, sem quaisquer restrições para tal;

c) sejam requisitado por determinação judicial ou governamental, desde que a AC ONLINE BRASIL e as ARs vinculadas comuniquem previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

2.8.3.3 Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC ONLINE BRASIL e as ARs vinculadas, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

2.8.4. Divulgação de informação de revogação/suspensão de certificado

2.8.4.1. A AC ONLINE BRASIL disponibiliza a lista de certificados revogados em seu repositório, http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/. Os motivos que justificaram a revogação são mantidos confidenciais pela AC ONLINE BRASIL e pelas ARs vinculadas, exceto quando:

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

b) esses motivos tenham sido publicados 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 ONLINE BRASIL ou das ARs vinculadas;

c) tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC ONLINE BRASIL ou ARs vinculadas, 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 ONLINE BRASIL 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 AC ONLINE BRASIL ou das ARs vinculadas, 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 previstos no 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 ONLINE BRASIL (eletrônicos ou não), pertencem e continuarão sendo de propriedade da AC ONLINE BRASIL. Direitos sobre Identificadores de Objeto (OID) atribuídos à AC ONLINE BRASIL 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. As ARs vinculadas à AC ONLINE BRASIL, utilizarão 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 individuo: comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado ou como representante legal de uma pessoa jurídica é realmente aquela cujos dados constam na documentação apresentada; vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil.

ii. confirmação da identidade de uma organização: comprovação de que os documentos apresentados 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) Verificação da solicitação de certificado - confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:

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

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

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

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

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

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

3.1.1.4. Será mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias 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;

3.1.2. Tipos de nomes

3.1.2.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "*distinguished name"* do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular. O certificado emitido para pessoa jurídica inclui o nome da pessoa física responsável. Para todos os efeitos legais, os certificados e as respectivas chaves de assinatura são de titularidade do responsável constante do certificado.

3.1.2.2. Não se aplica

3.1.3. Necessidade de nomes significativos

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

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Os identificadores "*Distinguished Name"* (DN) são únicos para cada entidade titular de certificado emitido pela AC ONLINE BRASIL. Números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo DN, conforme o padrão ITU X.509.

3.1.6. Procedimento para resolver disputa de nomes

A AC ONLINE BRASIL se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas.

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

3.1.8. Método para comprovar a posse de chave privada

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

3.1.9. Autenticação da Identidade de um Indivíduo

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

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

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

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

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

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

NOTA 4: Não se Aplica.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a CNH - Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

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

NOTA 7: Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

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

a) nome completo, sem abreviações[1];

1 No campo *Subject*, como parte do *Common Name*, que compõe o *Distinguished Name*

b) data de nascimento[2].

c) Não se Aplica.

3.1.9.2.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

a) Cadastro de Pessoa Física (CPF);

b) número de Identificação Social - NIS (PIS, PASEP ou CI);

c) número do Registro Geral - RG do titular e órgão expedidor;

d) número do Cadastro Especifico do INSS (CEI);

e) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;

f) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

g) documento assinado pela empresa com o valor do campo de login (UPN), quando aplicável.

3.1.9.2.3. Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original. Deve ser mantido arquivo com as cópias de todos os documentos utilizados.

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

NOTA 2: O cartão CPF poderá ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.10. Autenticação da Identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.1.1. Os procedimentos para confirmação da identidade de uma organização são os definidos a seguir.

2 No campo *Subject Alternative Name,* nas primeiras 8 (oito) posições do **OID 2.16.76.1.3.1**

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

a) relativos à 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 a sua habilitação fiscal:

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

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

3.1.10.3. Informações contidas no certificado emitido para uma organização:

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

a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;[3]

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);[4]

c) Nome completo do responsável pelo certificado, sem abreviações;[5]

d) Data de nascimento do responsável pelo certificado.[6]

3.1.10.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.1.9.2.

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Disposições Gerais

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

3.1.11.1.2. Se o titular for pessoa física, é feita a confirmação de sua identidade na forma do item 3.1.9.1. e essa assina o termo de titularidade de que trata o item 4.1.1.

3.1.11.1.3. Se o titular for pessoa jurídica, é feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

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

b) Apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;

c) Presença física 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, ou outorga de procuração atribuindo poderes para solicitação de certificado para equipamento ou aplicação e assinatura do respectivo termo de titularidade.

3 No campo Subject, como parte do Common Name, que compõe o Distinguished Name
4 No campo Subject Alternative Name, **OID 2.16.76.1.3.3**
5 No campo Subject Alternative Name, **OID 2.16.76.1.3.2**
6 No campo Subject Alternative Name, nas primeiras 8 (oito) posições do **OID 2.16.76.1.3.4**

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

3.1.11.2.1. Para certificados de equipamento ou aplicação que utilizem URL no campo Common Name, é verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele nome. Nesse caso é apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

3.1.11.2.2. Não se Aplica.

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

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

a) URL ou nome da aplicação;[7]

b) nome completo do responsável pelo certificado, sem abreviações;[8]

c) data de nascimento do responsável pelo certificado;[9]

d) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[10], se o titular for pessoa jurídica;

e) Cadastro Nacional de Pessoa Jurídica (CNPJ)[11], se o titular for pessoa jurídica.

3.1.11.3.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de responsabilidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.1.9.2.

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.

7 No campo *Subject*, como parte do *Common Name,* que compõe o *Distinguish Name*
8 No campo *Subject Alternativa Name,* OID **2.16.76.1.3.2**
9 No campo *Subject Alternativa Name,* nas primeiras 8 (oito) posições do OID **2.16.76.1.3.4**
10 No campo *Subject Alternativa Name, OID **2.16.76.1.3.8***
11 No campo *Subject Alternativa Name,* OID **2.16.76.1.3.3**

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

3.2.2. Esse processo citado acima é conduzido segundo uma das seguintes possibilidades:

a) Adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;
b) A solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva;
c) Em caso de pessoa jurídica, qualquer alteração em sua constituição e funcionamento deverá constar do processo de renovação.

3.2.3 Não se aplica.

3.3. 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 mesmo exigidos na solicitação inicial do certificado, na forma e prazo descritos nas PCs implementadas.

3.3.2 Não se aplica.

3.4. SOLICITAÇÃO DE REVOGAÇÃO

3.4.1 A solicitação de revogação de certificado é realizada por meio de formulário específico, permitindo a identificação inequívoca do solicitante, conforme descrito no item 4.4.3.

3.4.2 A confirmação a identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação com os dados fornecidos na solicitação de emissão.

4. REQUISITOS OPERACIONAIS

4.1. SOLICITAÇÃO DE CERTIFICADO

4.1.1. Neste item da DPC são descritos os requisitos e procedimentos operacionais estabelecidos pela AC ONLINE BRASIL e pelas ARs vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos compreendem:

a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.1;
b) a autenticação, mediante o uso de certificado digital do tipo A3, do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; e
c) a assinatura, pelo titular do certificado e pelo responsável pelo uso do certificado, no caso de pessoa jurídica, de termo de titularidade no modelo adendo referente ao TERMO DE TITULARIDADE específico.

4.1.2. Não se aplica.

4.1.3. Não se aplica.

4.1.4. Não se aplica.

4.2. EMISSÃO DE CERTIFICADO

4.2.1. Após os procedimentos de que trata o item 4.1.1, a AC ONLINE BRASIL realiza a emissão do certificado em seu sistema e notifica o titular por e-mail indicando o método para a retirada do certificado.

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

4.3. ACEITAÇÃO DE CERTIFICADO

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

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

4.3.2. A aceitação de todo certificado emitido é declarada implicitamente pelo titular na primeira utilização do certificado.

4.3.3 Não se aplica.

4.4. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1. Circunstâncias para revogação

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

4.4.1.2. Um certificado é obrigatoriamente revogado:

a) quando constatada emissão imprópria ou defeituosa do mesmo;

b) quando for necessária a alteração de qualquer informação constante no mesmo;

c) no caso de extinção, dissolução ou transformação da AC ONLINE BRASIL;

d) no caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;

e) no caso de falecimento do titular - pessoas físicas;

f) no caso de mudança na razão ou denominação social do titular - equipamentos, aplicações e pessoas jurídicas;

g) no caso de extinção, dissolução ou transformação do titular do certificado - equipamentos, aplicações e pessoas jurídicas;

h) no caso de falecimento ou demissão do responsável - equipamentos, aplicações e pessoas jurídicas; ou

i) por decisão judicial.

4.4.1.3. Observa-se ainda que:

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

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

4.4.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser solicitada:

a) pelo titular do certificado;

b) pelo responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;

c) pela empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;

d) pela AC ONLINE BRASIL;

e) por uma AR vinculada;

f) por determinação do CG da ICP-Brasil ou da AC Raiz;

g) Não se Aplica;

h) por decisão judicial.

4.4.3. Procedimento para solicitação de revogação

4.4.3.1. A AC ONLINE BRASIL garante que todos os habilitados, conforme o item 4.4.2. podem, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados.

4.4.3.1.1 A solicitação de revogação é encaminhada à AC ONLINE BRASIL por meio de formulário on-line, disponibilizado na página web http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil-inf/. Para tanto, o Titular ou Responsável deve fornecer os dados do certificado e a frase de identificação indicada na solicitação de emissão do certificado, bem como informar o motivo da revogação.

4.4.3.1.2 Caso o Titular ou o Responsável não se recorde da frase de identificação, o formulário de revogação deve ser impresso, assinado e entregue pessoalmente em uma das instalações técnicas da AR onde, foi realizada a validação presencial.

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 serão 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. O prazo máximo admitido para a conclusão do processo de revogação dos certificados emitidos pela AC ONLINE BRASIL, após o recebimento da respectiva solicitação é de 12 (doze) horas.

4.4.3.4 Não se aplica.

4.4.3.5. A AC ONLINE BRASIL responde 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 ONLINE BRASIL.

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 ONLINE BRASIL.

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 ONLINE BRASIL.

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 ONLINE BRASIL.

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 ONLINE BRASIL

4.4.9.2. A frequência máxima para emissão da LCR é de 6 (seis) horas.

4.4.9.3. Não se aplica.

4.4.9.4. Não se aplica.

4.4.10. Requisitos para verificação de LCR

4.4.10.1. Todo certificado deve ter a sua validade verificada, na respectiva LCR, 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*

O processo de revogação on-line está disponível ao Titular do Certificado, conforme descrito no item 4.4.3.

AC ONLINE BRASIL dispõe de recursos para verificação de *status on-line* de certificados, quando aplicável por força de contratação específica. A verificação da situação de um certificado poderá ser feita diretamente na AC ONLINE BRASIL, por meio do protocolo OCSP (On-line Certificate Status Protocol).

4.4.12. Requisitos para verificação de revogação on-line

Não se aplica.

4.4.13. Outras formas disponíveis para divulgação de revogação

Não se aplica.

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

Não se aplica.

4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deve notificar imediatamente a AC ONLINE BRASIL, solicitando a revogação de seu certificado, através do formulário específico para tal fim. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.4.15.2 O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente numa das instalações técnicas onde realizou a validação presencial, assinando formulário de solicitação de revogação, observado o previsto no item 4.4.3.

4.4.15.3 Todos os documentos e relatórios relativos a esse processo são arquivados após sua conclusão.

4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1. Tipos de Evento Registrados

4.5.1.1. A AC ONLINE BRASIL 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 ONLINE BRASIL;

c) mudanças na configuração da AC ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL 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. A AC ONLINE BRASIL não registra outras informações, além das descritas acima.

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 ONLINE BRASIL é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil [8].

4.5.1.6. As AR vinculadas à AC ONLINE BRASIL registram eletronicamente em

arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

a) os agentes de registro que realizaram as operações;

b) data e hora das operações;

c) a associação entre os agentes que realizaram a validação e aprovação e o certificado gerado;

d) a assinatura digital do executante.

4.5.1.7. A AC ONLINE BRASIL define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação

apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

4.5.2. Frequência de auditoria de registros (logs)

A análise dos registros de auditoria é realizada semanalmente pela Área de Segurança e PKI da AC ONLINE BRASIL. 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 ONLINE BRASIL 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 ONLINE BRASIL, 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. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção, através das funcionalidades nativas dos sistemas operacionais.

4.5.4.2. A inspeção contínua dos diversos registros dos sistemas é feita por meio de ferramentas nativas do sistema operacional e do banco de dados. Os relatórios emitidos a partir dessas ferramentas são coletados e armazenados em sala de arquivos em 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

São executados semanalmente os procedimentos de *backup* dos registros de auditoria dos sistemas utilizados pela AC ONLINE BRASIL. As cópias de segurança semanais

são feitas automaticamente ou pelos administradores de sistemas e enviadas as Equipe de Segurança e PKI.

4.5.6. Sistema de coleta de dados de auditoria

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

4.5.7. Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC ONLINE BRASIL 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 ONLINE BRASIL. 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 ONLINE BRASIL são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

4.6. ARQUIVAMENTO DE REGISTROS

4.6.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC ONLINE BRASIL:

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 ONLINE BRASIL;

g) informações de auditoria previstas no item 4.5.1;

4.6.2. Período de retenção para arquivo

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

a) as LCRs e os certificados de assinatura digital emitido pela AC ONLINE BRASIL 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, 6 (seis) anos.

4.6.3. Proteção de arquivos

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da ICP-Brasil. Mídias de arquivos são guardadas em local seguro. 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 ONLINE BRASIL, 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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC e pelo pessoal operacional.

4.6.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC ONLINE BRASIL, 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. Trinta dias antes da expiração do certificado digital, a AC ONLINE BRASIL ou a AR vinculada, através do e-mail cadastrado no formulário de solicitação de certificado, informa ao titular a data de expiração e as instruções para a solicitação de um novo certificado.

4.7.2. Não se aplica.

4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

Os procedimentos de notificação e de recuperação de desastres, para garantir a continuidade dos serviços críticos, estão descritos no Plano de Continuidade de Negócio (PCN) da AC ONLINE BRASIL. Esse PCN, de caráter sigiloso, é testado pelo menos uma vez por ano.

4.8.1. Recursos computacionais, *software* ou dados corrompidos

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 ONLINE BRASIL.

4.8.2. Certificado de entidade revogado

O PCN especifica as ações a serem tomadas no caso em que o certificado da AC ONLINE BRASIL for revogado, as quais se resumem no seguinte:

a) em caso de revogação do certificado da AC ONLINE BRASIL, 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 todos os certificados emitidos pela das AC ONLINE BRASIL. É gerado novo par de chaves da AC ONLINE BRASIL, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado. A AC ONLINE BRASIL emite então novos certificados digitais para os usuários finais que tiveram seus certificados revogados nesta situação.

4.8.3. Chave de entidade comprometida

O PCN especifica as ações a serem tomadas no caso em que a chave privada da AC ONLINE BRASIL for comprometida, e que se resumem no seguinte:

a) em caso de comprometimento da chave da AC ONLINE BRASIL, 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 ONLINE BRASIL e os certificados por ela emitidos. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado da AC ONLINE BRASIL. A seguir são emitidos, pela AC ONLINE BRASIL, novos certificados digitais para os usuários finais que tiveram seus certificados revogados nesta situação.

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

4.8.4.1. O PCN especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza, como fogo, greves etc. e que podem ser resumidas no seguinte:

a) é feita a identificação da crise e o acionamento das equipes envolvidas;

b) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas;

c) confirmado o desastre e constatada a impossibilidade de operação no site principal, as atividades são transferidas para o site de contingência.

4.8.5. Atividades das Autoridades de Registro

O PCN das ARs Vinculadas contempla os procedimentos para recuperação total ou parcial das atividades da AR, 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, AR ou PSS

4.9.1. A AC ONLINE BRASIL 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 ONLINE BRASIL ou de ARs vinculadas, 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) extinguir a emissão, revogação e publicação de LCR e/ou dos serviços de status on-line, após a revogação de todos os certificados emitidos;

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 ONLINE BRASIL e AR ONLINE CERTIFICADORA;

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 ONLINE BRASIL 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 ONLINE BRASIL não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Nas instalações da AC ONLINE BRASIL, foram implementados, entre outros, os seguintes controles de segurança física:

a) 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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL, 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 ONLINE BRASIL. 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 ONLINE BRASIL transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC ONLINE BRASIL 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 ONLINE BRASIL, 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 ONLINE BRASIL.

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 ONLINE BRASIL. 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 ONLINE BRASIL, 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 ONLINE BRASIL, 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 ONLINE BRASIL 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 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 obedece às seguintes especificações:

a) é feito em aço;

b) possui tranca com chave.

5.1.2.1.14. **O sexto nível – ou nível 6** - consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da AC ONLINE BRASIL estão armazenados nesses 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, são permanentemente monitorados por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmaras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.2.3. Sistema de Controle de Acesso

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

5.1.2.4. Mecanismos de emergência

5.1.2.4.1. Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL e seus respectivos serviços. Um sistema de aterramento está implantado.

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

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

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

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

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

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

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

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

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

a) geradores de porte compatível;

b) geradores de reserva;

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

d) sistemas redundantes de ar condicionado.

5.1.4. Exposição à água

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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL, 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 ONLINE BRASIL 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 documentadas 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

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

5.2. CONTROLES PROCEDIMENTAIS

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

5.2.1. Perfis qualificados

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

5.2.1.2. A AC ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL, 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 ONLINE BRASIL necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC ONLINE BRASIL. 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 ONLINE BRASIL passam por um processo rigoroso de seleção. Todo funcionário da AC ONLINE BRASIL tem sua identidade e perfil verificados antes de:

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

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

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

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

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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL e pelas ARs vinculadas 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 ONLINE BRASIL e das ARs vinculadas, 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 ONLINE BRASIL;

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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL e da AR vinculada;

b) sistema de certificação em uso na AC ONLINE BRASIL;

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 ONLINE BRASIL e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC ONLINE BRASIL e no sistema das ARs.

5.3.5. Frequência e sequência de rodízios de cargos

A AC ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL e da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC ONLINE BRASIL e das AR, 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 ONLINE BRASIL.

5.3.8. Documentação disponibilizada ao pessoal

5.3.8.1. A AC ONLINE BRASIL disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas:

a) esta DPC;

b) as PC que implementa;

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 ONLINE BRASIL.

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

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1. Geração do Par de Chaves

6.1.1.1. O par de chaves da AC ONLINE BRASIL é gerado pela própria AC ONLINE BRASIL em módulo criptográfico de hardware, com padrão de segurança FIPS 140-2 nível 3 (para cadeia de certificação V2 e V3) conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.1.2. Pares de chaves são gerados somente pelo titular do certificado correspondente.

6.1.1.3. As PCs implementadas pela AC ONLINE BRASIL definem o meio utilizado para armazenamento da chave privativa, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável, pois é responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

6.1.3. Entrega da chave pública para emissor de certificado

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

6.1.3.2. Chaves públicas de usuários finais são entregues à AC ONLINE BRASIL por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC ONLINE BRASIL. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4. Disponibilização de chave pública da AC ONLINE BRASIL para usuários

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC ONLINE BRASIL 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* www.onlinecertificadora.com.br

c) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

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

6.1.5.2. Não se aplica.

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC ONLINE BRASIL adotam o padrão FIPS 140-2 nível 3 (para as cadeias de certificação V2 e V3), 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. Para geração de seus pares de chaves, a AC ONLINE BRASIL utiliza componentes seguros de *hardware,* que possuem mecanismos de prevenção e detecção de violação.

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

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

6.1.9.1. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC ONLINE BRASIL, bem como as possíveis

restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC implementada.

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

6.2. PROTEÇÃO DA CHAVE PRIVADA

As chaves privadas da AC ONLINE BRASIL 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. AC ONLINE BRASIL adota o padrão de homologação da ICP-Brasil NSH-2, conforme disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Nos certificados de titulares finais, esses devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]. Cada PC implementada especifica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.2.2. Controle “n de m’ para chave privada

6.2.2.1. A chave criptográfica de ativação do componente seguro de *hardware* que armazena a chave privada da AC ONLINE BRASIL é dividida em 8 (oito) partes e distribuídas por 8 (oito) custodiantes designados pela AC ONLINE BRASIL (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, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. Cópia de segurança (*backup*) de chave privada

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

6.2.4.2. A AC ONLINE BRASIL 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 ONLINE BRASIL não mantém cópia de segurança das chaves privadas de certificado de assinatura digital por ela emitido. Cada PC implementada define os requisitos específicos aplicáveis.

6.2.4.4. A cópia de segurança deverá ser armazenada, cifrada, por algoritmo simétrico como 3-DES e AES 256 conforme 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 ONLINE BRASIL 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 AC ONLINE BRASIL gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

6.2.7. Método de ativação de chave privada

A ativação das chaves privadas da AC ONLINE BRASIL é implementada por meio do módulo criptográfico, após identificação dos operadores responsáveis. Esta identificação é realizada por meio de senha e de 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 ONLINE BRASIL. Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

6.2.8. Método de desativação de chave privada

6.2.8.1 A chave privada da AC ONLINE BRASIL, 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.

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

6.2.9. Método de destruição de chave privada

Quando a chave privada da AC ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL.

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. Arquivamento de chave pública

As chaves públicas da própria AC ONLINE BRASIL e dos titulares dos certificados por ela emitidos, bem como as LCR emitidas, serão armazenados pela AC ONLINE BRASIL, 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 ONLINE BRASIL 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. . Cada PC implementada pela AC ONLINE BRASIL define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL [7].

6.3.2.4 A validade admitida para certificados AC ONLINE BRASIL é limitada pela validade do certificado da AC VALID.

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 ONLINE BRASIL são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em *hardware (*cartão criptográfico*)*.

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

6.4.2. Proteção dos dados de ativação.

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

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

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A AC ONLINE BRASIL 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 onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC ONLINE BRASIL são descritos em cada PC implementada.

6.5.1.3. Os computadores servidores, utilizados pela AC ONLINE BRASIL, 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 ONLINE BRASIL;

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

c) acesso restrito aos bancos de dados da AC ONLINE BRASIL;

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 ONLINE BRASIL;

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 ONLINE BRASIL 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 ONLINE BRASIL. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC ONLINE BRASIL 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 ONLINE BRASIL 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 ONLINE BRASIL.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1. A AC ONLINE BRASIL implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas ARs Vinculadas para os processos de validação e aprovação de certificados.

6.5.3.2. São incluídos, no mínimo, os requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARS DA ICP-BRASIL [1], tais como:

a) Segurança de Pessoal:

b) Segurança Física;

c) Segurança Lógica;

d) Segurança de Rede; e

e) Segurança da Informação.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1. A AC ONLINE BRASIL 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, a gerência de infraestrutura da AC ONLINE BRASIL avalia e decide quando será a implementação no ambiente de produção.

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

6.6.2. Controle de gerenciamento de segurança

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

a) a AC ONLINE BRASIL opera em equipamento fisicamente protegido em ambiente de nível 4;

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 ONLINE BRASIL, 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 ONLINE BRASIL 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 ONLINE BRASIL, incluindo firewalls e recursos similares.

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

6.7.1.3. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls, e sistemas de detecção de intrusos (IDS),

localizados no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4.

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

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

6.7.2. Firewall

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

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 pela AC ONLINE BRASIL para o armazenamento de sua chave privada adota o padrão de homologação da ICP-Brasil NSH-2. Este padrão está 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 ONLINE BRASIL.

7.1.2. A AC ONLINE BRASIL implementa as PCs abaixo, as quais especificam os formatos dos certificados gerados e das correspondentes LCR. Nessas PC são incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

Política de Certificado	Nome	OID
Política de Certificado de Assinatura Digital do tipo A1 da AC ONLINE BRASIL	PC A1 da AC ONLINE BRASIL	2.16.76.1.2.1.48
Política de Certificado de Assinatura Digital do tipo A3 da AC ONLINE BRASIL	PC A3 da AC ONLINE BRASIL	2.16.76.1.2.3.45

7.1.3. Não se aplica.

7.2. PERFIL DO CERTIFICADO

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

7.2.2. Extensões de certificados

Não se aplica.

7.2.3. Identificadores de Algoritmo

Não se aplica.

7.2.4. Formatos de nome

Não se aplica.

7.2.5. Restrições de nome

Não se aplica.

7.2.6. OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC ONLINE BRASIL após conclusão do processo de seu credenciamento, é **2.16.76.1.1.61**.

7.2.7. Uso da extensão “Policy Constraints”

Não se aplica.

7.2.8. Sintaxe e semântica dos qualificadores de política

Não se aplica.

7.2.9. Semântica de processamento para extensões criticas.

Não se aplica.

7.3. Perfil de LCR

7.3.1. Número (s) de versão

As LCR geradas pela AC ONLINE BRASIL 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 ONLINE BRASIL adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) **"*Authority Key Identifier*", não crítica:** contém o resumo SHA-1 da chave pública da AC ONLINE BRASIL que assina a LCR;

b) "**C*RL Number*", não crítica**: contém número sequencial para cada LCR emitida.

c) "***Authority Information Access***", não crítica: contém o método de acesso id-ad-caIssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/ac-onlinebrasilv2.p7b

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

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

8.2. POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO

A AC ONLINE BRASIL pública e mantém atualizada está DPC, em seu endereço web:

http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/dpc-ac-onlinebrasil.pdf

8.3. PROCEDIMENTOS DE APROVAÇÃO

Esta DPC foi submetida à aprovação da AC-RAIZ da ICP-Brasil, durante o processo de credenciamento da AC ONLINE BRASIL, 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

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