DOCCLOUD
CERTIFICADO DIGITAL

Declaração de Práticas de Certificação da AC DOCCLOUD
DPC da AC DOCCLOUD

OID: 2.16.76.1.1.81
Versão 3.0

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

CONTROLE DE ALTERAÇÕES

RESPONSÁVEL	APROVAÇÃO	DESCRIÇÃO DA ALTERAÇÃO	VERSÃO	DATA
Compliance	Resolução nº 197, de 16.11.2021 Versão 6.2	Regulamentação dos procedimentos e requisitos técnicos para a operacionalização de Autoridade de Registro Eletrônica na ICP-Brasil.	3.0	12.09.2022
Compliance	Resoluções 177/2020 e 181/2021 Versão 6.1	Atualização das informações conforme resoluções	2.0	01.09.2021
Compliance	Versão Inicial		1.0	03.12.2020

1. INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

1.1. VISÃO GERAL

1.1.1. Esta Declaração de Práticas de Certificação – DPC, descreve as práticas e os procedimentos empregados pela Autoridade Certificadora DOCCLOUD - AC DOCCLOUD, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil e descreve as práticas e os procedimentos utilizados pela AC DOCCLOUD na execução de seus serviços de certificação digital.

1.1.2. Esta Declaração de Práticas de Certificação – DPC, adota obrigatoriamente a estrutura e requisitos empregados pelo documento: Requisitos Mínimos para as Declaração de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil – DOC-ICP-05, em sua versão 6.1.

1.1.3. Item não aplicável.

1.1.4. A estrutura desta DPC da AC DOCCLOUD está baseada nas resoluções do Comitê Gestor da ICP-Brasil (CG ICP-Brasil) e na RFC 3647.

1.1.5. A AC DOCCLOUD mantém atualizada esta Declaração de Práticas de Certificação de acordo com as resoluções do Comitê Gestor da ICP-Brasil.

1.1.6. Esta Declaração de Práticas de Certificação está em conformidade com o conjunto normativo da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.

1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1. Este documento é chamado “Declaração de Práticas de Certificação da Autoridade Certificadora DOCCLOUD” e comumente referido como “DPC da AC DOCCLOUD”. O Identificador de Objeto **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.81.**

1.2.2. Item não aplicável.

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. Autoridades Certificadoras

Esta DPC refere-se exclusivamente à Autoridade Certificadora DOCCLOUD - AC DOCCLOUD de 1º nível no âmbito da ICP-Brasil e encontra-se publicada no seu repositório, no seguinte endereço:
http://repositorio.acdoccloud.com.br/ac-doccloud/dpc-acdoccloud.pdf

1.3.2. Autoridades de Registro

1.3.2.1. A Autoridade de Registro (AR) é uma entidade que desempenha o papel de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação dos seus solicitantes em nome da AC.

As ARs vinculadas à AC de nível subsequente à AC DOCCLOUD estão relacionadas na URL www.doccloud.com.br/repositorios/acdoccloud com as seguintes informações:

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

1.3.3. Titulares de Certificado

Apenas pessoas jurídicas podem ser titulares de certificados de AC Subsequente emitidos pela AC DOCCLOUD.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

1.3.5.1. A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC DOCCLOUD é publicada em serviço de diretório e/ou em página web da AC DOCCLOUD: www.doccloud.com.br/repositorios/acdoccloud

1.4. USABILIDADE DO CERTIFICADO

1.4.1. Uso apropriado do certificado

Os certificados emitidos pela AC DOCCLOUD tem sua utilização exclusiva para assinatura de certificados digitais de AC de nível imediatamente subsequente (AC Subsequente) ao seu e de sua Lista de Certificados Revogados (LCR).

1.4.2. Uso proibitivo do certificado

Os certificados emitidos pela AC DOCCLOUD devem apenas ser usados na medida em que seja consistente com a lei aplicável.

1.5. POLÍTICA DE ADMINISTRAÇÃO

1.5.1. Organização administrativa do documento

AC DOCCLOUD
DOCCLOUD SOLUCAO DIGITAL

1.5.2. Contatos

Endereço: Rua Gonçalves Dias, 519 – Jardim Girassol - Americana/SP - CEP: 13.465-670.
Telefone: (19) 3477-1144
Página Web: www.doccloud.com.br
E-mail: compliance@doccloud.com.br

1.5.3. Adequabilidade das DPC's com PC's

AC DOCCLOUD
Nome: Lucas Carvalho dos Santos
Departamento: NORMAS & COMPLIANCE
Telefone: (19) 3477-1144
E-mail: lucas.santos@doccloud.com.br

1.5.4. Procedimentos de aprovação desta DPC

Este documento foi analisado pela alta gestão da AC DOCCLOUD e submetido ao Instituto de Tecnologia da Informação – ITI para aprovação. Os procedimentos de aprovação da DPC da AC são estabelecidos a critério do CG da ICP-Brasil.

1.6. DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
CSR	Certificate Signing Request
DETRAN	Departamento Nacional de Trânsito
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSBIO	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestador de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria

TLS	Transport Layer Security
TSDM	Trusted Software Development Methodology
TSE	Tribunal Superior Eleitoral
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. REPOSITÓRIOS

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

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

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

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

2.1.2. O repositório da AC DOCCLOUD está disponível para consulta pública, através de protocolo http:

A disponibilidade das informações publicadas pela AC DOCCLOUD em serviço de repositório e/ou página web é de 99,5% (noventa e nove virgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

Não há qualquer restrição ao acesso para consulta ao repositório.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não-autorizado.

Somente a AC DOCCLOUD, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar atualizações nas informações por ela publicadas no seu repositório

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

2.1.4 A AC DOCCLOUD disponibiliza 2 (dois) repositórios em infraestrutura de rede segregadas para distribuição de LCR, nos endereços:

1. http://repositorio.acdoccloud.com.br/ac-doccloud/lcr-ac-doccloud.crl

2. http://repositorio2.acdoccloud.com.br/ac-doccloud/lcr-ac-doccloud.crl

2.2. PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICADOS

2.2.1. A AC DOCCLOUD publica e disponibiliza informações, tais como certificados, LCR, sua DPC, entre outras, em página WEB, com disponibilidade de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.2. As seguintes informações são publicadas na página web da AC DOCCLOUD em: www.doccloud.com.br/repositorios/acdoccloud

a) os certificados da AC DOCCLOUD;
b) suas LCR's;
c) sua DPC;
d) Item não aplicável;
e) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.3.1. A AC DOCCLOUD atualiza as informações descritas no item anterior logo que sejam geradas, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos. Os certificados são publicados após emissão.

A LCR é publicada de acordo com o disposto no item 4.9.7, 4.9.8 e 4.10 desta DPC.

2.4. CONTROLE DE ACESSO AOS REPOSITÓRIOS

2.4.1. Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC DOCCLOUD.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. ATRIBUIÇÕES DE NOMES

3.1.1. Tipos de nomes

3.1.1.1. Os identificadores “Distinguished Name” (DN) são únicos para cada AC de nível imediatamente subsequente ao da AC DOCCLOUD. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.500, endereços de correio eletrônico ou endereços de página web (URL).

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

3.1.2. Necessidade de nomes serem significativos

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

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

Item não aplicável.

3.1.4. Regras para interpretação de vários tipos de nomes

3.1.4.1. Item não aplicável.

3.1.4.2. É vedado o uso de nomes nos certificados que violem os direitos de propriedade intelectual de terceiros

3.1.5. Unicidade de nomes

Os identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC DOCCLOUD. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo DN

Para assegurar a unicidade do campo DN podem ser incluídos números ou letras adicionais ao nome de cada titular.

3.1.6. Procedimento para resolver disputa de nomes

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

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

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

3.2. VALIDAÇÃO INICIAL DE IDENTIDADE

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

a) IDENTIFICAÇÃO DO TITULAR DO CERTIFICADO – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3:

i. Confirmação da Identidade de um Indivíduo: item não aplicável.

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

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

3.2.1. Método para comprovar o controle de chave privada

A AC DOCCLOUD verifica se a entidade que solicita o certificado controla a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. O descrito no RFC 4210, atualizada pela RFC 6712 é utilizado como referência para essa finalidade.

3.2.2. Autenticação da identidade de uma organização

3.2.2.1. Disposições Gerais

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

3.2.2.1.2. 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.

3.2.2.1.3. A confirmação da identidade da organização e da pessoa física responsável pelo certificado nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.2.2.2;
b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;
c) coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil, bem como os procedimentos para identificação biométrica na ICP-Brasil; e
d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo responsável pelo uso do certificado.

NOTA 1: Poderá a AC DOCCLOUD solicitar uma assinatura manuscrita ao titular ou responsável pelo uso do certificado para comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

3.2.2.1.4. Item não aplicável.

3.2.2.1.5. O disposto no item 3.2.2.1.3 poderá ser realizado:

a) mediante comparecimento presencial do responsável pelo certificado.

3.2.2.2. Documentos para efeitos de identificação de uma organização

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

a) Relativos 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) Certidão Simplificada emitida pela Junta Comercial ou Ato Constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e
2) Documentos da eleição de seus administradores, quando aplicável;

b) Item não aplicável.

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

3.2.2.3. Informações contidas no certificado emitido para uma organização

3.2.2.3.1. Item não aplicável.

3.2.2.3.2. Item não aplicável.

3.2.2.4. Responsabilidade decorrente do uso do certificado de uma organização

Item não aplicável.

3.2.3. Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo responsável pela AC de nível imediatamente subsequente ao da AC DOCCLOUD é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos

3.2.3.1. Documentos para efeitos de identificação de um indivíduo

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

A identificação da pessoa física requerente do certificado deverá ser realizada como segue:

a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:

i. Registro de Identidade, se brasileiro; ou
ii. Título de eleitor com foto; ou

iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou
iv. Passaporte, se estrangeiro não domiciliado no Brasil.

b) Item não aplicável

Nota 1: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia, em caso de documento pouco legíveis a AC DOCCLOUD, reserva-se ao direito de solicitar mais do que um documento de identificação.

3.2.3.1.1 Item não aplicável.

3.2.3.1.2 Item não aplicável.

3.2.3.1.3 Item não aplicável.

3.2.3.1.4 Item não aplicável.

3.2.3.1.5 Item não aplicável.

3.2.3.1.6 Item não aplicável.

3.2.3.1.7 Item não aplicável.

3.2.3.1.8 Item não aplicável.

3.2.3.1.8.1 Item não aplicável.

3.2.3.2. Informações Contidas no Certificado Emitido para um Individuo.

Item não aplicável.

3.2.4 Informações não verificadas do titular do certificado

Item não aplicável.

3.2.5 Validação das autoridades

Na emissão de certificado de AC subsequente é verificado se a pessoa física é o representante legal da AC.

3.2.6 Critérios para interoperação

Item não aplicável.

3.2.7 Autenticação da identidade de equipamento ou aplicação

Item não aplicável.

3.2.8 Procedimentos complementares

3.2.8.1 À AC DOCCLOUD mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro.

3.2.8.2 Item não aplicável.

3.2.8.3 É mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias são mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.1. Item não aplicável.

3.2.8.3.2. Item não aplicável.

3.2.8.4. Item não aplicável.

3.2.8.4.1. Item não aplicável.

3.2.8.4.2. Item não aplicável.

3.2.9 PROCEDIMENTOS ESPECÍFICOS

Item não aplicável.

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

3.3.1 Esta DPC estabelece os processos de identificação e confirmação do cadastro do solicitante pela AC DOCCLOUD para a geração de novo par de chaves, e de seu correspondente certificado.

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

a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3.
b) Item não aplicável;
c) Item não aplicável;
d) Item não aplicável;
e) Item não aplicável;

3.3.2.1 Item não aplicável

3.3.3. Item não aplicável.

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

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado é realizada através de declaração assinada pelo(s) representante(s) legal(is) com firma(s) reconhecida(s).

O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3. Solicitações de revogação de certificados devem ser registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 SOLICITAÇÃO DO CERTIFICADO

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

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.2;
b) item não aplicável;
c) item não aplicável.

4.1.1 Quem pode submeter uma solicitação de certificado

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

4.1.1.1 A emissão de um certificado pela AC DOCCLOUD é feita em cerimônia específica, com a presença dos representantes da AC DOCCLOUD, da AC habilitada, convidados e testemunhas, na qual são registrados todos os procedimentos executados. Todos estes procedimentos serão realizados somente após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.1.2 Item não aplicável.

4.1.1.3 Nos casos previstos no item 4.1.1.1, à AC subsequente deverá encaminhar a solicitação de certificado à AC DOCCLOUD por meio de seus Representantes Legais, utilizando o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

4.1.1.4 O certificado de AC de nível imediatamente subsequente à AC DOCCLOUD deve ser feita por seus Representantes Legais. A AC DOCCLOUD garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 10 (dez) dias úteis após o recebimento da solicitação.

4.1.2 Processo de registro e responsabilidades

4.1.2.1 Responsabilidades da AC

4.1.2.1.1 A AC DOCCLOUD responde pelos danos a que der causa.

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

4.1.2.1.3 Item não aplicável.

4.1.2.2 Obrigações da AC DOCCLOUD

As obrigações da AC DOCCLOUD são as abaixo relacionadas:

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

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

4.1.2.3 Responsabilidades da AR
A AR será responsável pelos danos a que der causa.

4.1.2.4 As obrigações das AR
Item não aplicável.

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1 Execução das funções de identificação e autenticação

À AC DOCCLOUD e a AR DOCCLOUD executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2 Aprovação ou rejeição de pedidos de certificado

4.2.2.1 À AC DOCCLOUD pode aceitar ou rejeitar pedidos de certificados das AC imediatamente subsequente de acordo com os procedimentos descritos no item 4.1 desta DPC.

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

4.2.3 Tempo para processar a solicitação de certificado

À AC DOCCLOUD cumpre os procedimentos determinados na ICP-Brasil. Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3 EMISSÃO DE CERTIFICADO

4.3.1 Ações da AC DOCCLOUD durante à emissão de um certificado

4.3.1.1 Realizada a validação da solicitação do certificado, de que trata o item 3.2, a AC DOCCLOUD procede à emissão do certificado. O certificado emitido é inserido na relação de certificados emitidos pela AC DOCCLOUD e uma cópia do certificado é entregue ao representante da AC.

4.3.1.2 A aceitação de todo certificado emitido é garantida pela assinatura do Termo de Responsabilidade emitido pela AC DOCCLOUD para AC Titular.

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

A notificação de emissão é feita através da assinatura dos seguintes documentos:
a) Termo de Cerimônia de Geração de Chaves;
b) Formulário de Solicitação de Emissão de Certificado;
c) Termo de Titularidade de Certificado;
d) Termo de Cerimônia de Emissão de Certificado; e
e) Termo de Acordo (no qual a AC subsequente atesta ter recebido o seu certificado).

4.4 ACEITAÇÃO DE CERTIFICADO

4.4.1 Conduta sobre a aceitação do certificado

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

4.4.1.2 A aceitação do certificado de uma AC subsequente é declarada por seu responsável.

4.4.1.3 Item não aplicavél.

4.4.2 Publicação do certificado pela AC DOCCLOUD

O certificado da AC e os certificados das ACs de nível imediatamente subsequente ao seu são publicados de acordo com item 2.2 desta DPC.

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

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

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

A AC subsequente titular de certificado emitido pela AC DOCCLOUD, deve operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementa, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1 Usabilidade da Chave privada e do certificado do titular

4.5.1.1 A AC DOCCLOUD utiliza sua chave privada e garanti a proteção dessa chave conforme o previsto na sua própria DPC.

4.5.1.2 Obrigações do Titular do Certificado

As obrigações das ACs titulares de certificados emitidos de acordo com esta DPC da AC DOCCLOUD 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 chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e
e) informar à AC DOCCLOUD qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

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

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.1 Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2 Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3 Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4 Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com item 3.3 desta DPC.

4.6.6 Publicação de uma renovação de um certificado pela AC

Item não aplicável

4.6.7 Notificação de emissão de certificado pela AC para outras entidades

Em acordo com item 4.3 desta DPC.

4.7 NOVA CHAVE DE CERTIFICADO (Re-key)

4.7.1 Circunstâncias para nova chave de certificado

Item não aplicável

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

Item não aplicável

4.7.3 Processamento de requisição de novas chaves de certificado

Item não aplicável

4.7.4 Notificação de emissão de novo certificado para o titular

Item não aplicável

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

Item não aplicável

4.7.6 Publicação de uma nova chave certificada pela AC

Item não aplicável

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

Item não aplicável

4.8 MODIFICAÇÃO DE CERTIFICADO

Item não aplicável

4.8.1 Circunstâncias para modificação de certificado

Item não aplicável

4.8.2 Quem pode requisitar a modificação de certificado

Item não aplicável

4.8.3 Processamento de requisição de modificação de certificado

Item não aplicável

4.8.4 Notificação de emissão de novo certificado para o titular

Item não aplicável

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

Item não aplicável

4.8.6 Publicação de uma modificação de certificado pela AC

Item não aplicável

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

Item não aplicável

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.9.1 Circunstâncias para revogação

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

4.9.1.2. 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 dissolução de AC titular do certificado; ou
d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.9.1.3 Esta DPC observa ainda que:

a) A AC DOCCLOUD revogará, no prazo definido no item 4.9.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
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 para a ICP-Brasil.

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

4.9.1.4.1 Item não aplicável.

4.9.1.4.2 Item não aplicável.

4.9.1.5 A AC DOCCLOUD observa a autenticidade da LCR/OCSP que também é confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR/ OCSP

4.9.2 Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

a) por solicitação da AC Titular do Certificado;
b) por determinação da AC DOCCLOUD;
c) por solicitação da AR DOCCLOUD;
d) por determinação do CG da ICP-Brasil;
e) por determinação da AC Raiz; ou
f) por determinação judicial.

4.9.3 Procedimento para solicitação de revogação.

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

4.9.3.2. Como diretrizes gerais, fica estabelecido que:

a) o solicitante da revogação de um certificado será identificado;
b) as solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;
c) as justificativas para a revogação de um certificado serão documentadas; e
d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado; e
e) A comunicação à AC afetada, quando a iniciativa de revogação partir da AC DOCCLOUD.

4.9.3.3 O prazo máximo para conclusão do processo de revogação do certificado pela AC DOCCLOUD, após a conclusão do processo de aceitação e registro da solicitação de revogação é de 24 (vinte e quatro) horas.

4.9.3.4 O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 24 (vinte e quatro) horas

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

4.9.3.6 Item não aplicável.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. 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 3 (três) dias úteis, dentro desse prazo a revogação do certificado pode ser solicitada sem ônus.

4.9.4.2. Item não aplicável.

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

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

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7 Frequência de emissão de LCR

4.9.7.1. A AC emite a LCR referente a certificados de AC subordinadas em um prazo máximo de 90 (noventa) dias.

4.9.7.2. Item não aplicável.

4.9.7.3. A frequência máxima admitida para a emissão de LCR referente a certificados de AC Subsequente é de 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente a AC DOCCLOUD, é emitida nova LCR no prazo previsto no item 4.9.3.4 e notificada a todas as AC de nível imediatamente subsequente ao seu.

4.9.7.4. Item não aplicável.

4.9.7.5 Item não aplicável.

4.9.8 Latência máxima para a LCR

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

4.9.9 Disponibilidade para revogação/verificação de status on-line

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

4.9.10 Requisitos para verificação de revogação on-line

Item não aplicável.

4.9.11 Outras formas disponíveis para divulgação de revogação

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

4.9.11.2 Item não aplicável

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. No caso do comprometimento da chave privada de uma AC de nível imediatamente subsequente ao da AC DOCCLOUD, essa notificará imediatamente à AC DOCCLOUD.

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

4.9.13 Circunstâncias para suspensão

No âmbito da ICP-Brasil, não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de AC de nível imediatamente subsequente ao da AC DOCCLOUD.

4.9.14 Quem pode solicitar suspensão

A AC DOCCLOUD, desde que aprovado pelo Comitê Gestor.

4.9.15 Procedimento para solicitação de suspensão

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

4.9.16 Limites no período de suspensão

Os períodos de suspensão serão estabelecidos por norma específica da DPC associada.

4.10 SERVIÇOS DE STATUS DE CERTIFICADO

4.10.1 Características operacionais

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

4.10.2 Disponibilidade dos serviços

Ver item 4.9

4.10.3 Funcionalidades operacionais

Ver item 4.9

4.11 ENCERRAMENTO DE ATIVIDADES

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

4.11.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC DOCCLOUD segue os requisitos e procedimentos descritos no documento Plano de Encerramento. Esse plano tem abordagem multidisciplinar envolvendo aspectos de várias áreas da companhia, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC DOCCLOUD:

a) Comunicará publicamente a extinção dos serviços da AC DOCCCLOUD, através de publicação em jornal de grande circulação.
b) Revogará todos os certificados gerados pela AC DOCCLOUD nos prazos estipulados nesta DPC, após a publicação e comunicará às partes afetadas através de mensagem eletrônica.
c) Extinguirá os serviços de emissão de certificados.
d) Extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços de status on-line após a revogação completa de todos os certificados.
e) Destruirá a chave privada da AC DOCCLOUD extinta seguindo o procedimento descrito na DPC Item 6.2.9.
f) Transferirá os dados e gravações da AC DOCCLOUD para a Autoridade Certificadora sucessora, aprovada pela AC Raiz. O período no qual eles ficarão armazenados está descrito na DPC item 4.6.
g) Transferirá as chaves públicas dos certificados emitidos pela AC DOCCLOUD para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC DOCCLOUD. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.
h) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC DOCCLOUD.
i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

No caso de encerramento das atividades como AR vinculada a AC DOCCLOUD a AR deverá seguir os seguintes requisitos e procedimentos:

a) Comunicará publicamente a extinção dos serviços de AR vinculada AC DOCCLOUD, através de

publicação em jornal de grande circulação.
b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados;
c) Ficará responsável pela guarda dos documentos, dados e registros relativos aos pedidos de emissão de certificados para a AC DOCCLOUD, devendo fornecê-los sempre que solicitada pelo Titular, ou pela AC DOCCLOUD. O período no qual eles ficarão armazenados está descrito na DPC item 4.6.

Em caso de falência ou extinção da AR a documentação e registros relativos à emissão de certificados deverá ser entregue para guarda da AC DOCCLOUD.

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

a) Publicará, em sua página web, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso;
b) Manterá a guarda de toda a documentação comprobatória em seu poder.

4.12 CUSTÓDIA E RECUPERAÇÃO DA CHAVE

4.12.1 Política e práticas de custódia e recuperação de chave

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

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

A AC DOCCLOUD não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1. Controles físicos

O acesso físico às dependências da AC DOCCLOUD 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 DOCCLOUD está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.1 Construção e localização das instalações de AC

5.1.1.1 A operação da AC DOCCLOUD 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 DOCCLOUD não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos. Nenhuma das linhas telefônicas dentro do ambiente de certificação da AC oferece suporte a modem.

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

a) As instalações para equipamentos de apoio, tais como maquinas de ar condicionado, nobreaks, baterias, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro, com entrada e saída controlada através de câmeras de monitoramento;
b) As instalações para sistemas de telecomunicações, quadros de distribuição de energia e de telefonia ficam em ambiente de nível 3 (três);
c) Existem sistemas de aterramento e de proteção contra descargas atmosféricas;
d) Existe iluminação de emergência em todos os níveis e áreas cobertas por câmeras de monitoramento.

5.1.2 Acesso físico

A AC DOCCLOUD inseriu um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a Política de Segurança implementada e os requisitos que seguem.

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 DOCCLOUD, 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 DOCCLOUD. 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 DOCCLOUD transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC DOCCLOUD 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 DOCCLOUD, 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 DOCCLOUD.

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 DOCCLOUD. 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 DOCCLOUD, 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 DOCCLOUD, 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 DOCCLOUD possui um único ambiente para abrigar os equipamentos de produção online, os

equipamentos de produção off-line, o cofre de armazenamento e os equipamentos de rede e infraestrutura (firewall, roteadores, switches e servidores).

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

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

a) ser feito em aço ou material de resistência equivalente;
b) possuir tranca com chave.

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

5.1.2.2. Sistema físico de detecção

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

5.1.2.2.2. As mídias de vídeo resultantes da gravação 24x7 são armazenadas por 7 (sete) anos. Elas são testadas (verificação de trechos aleatórios no início, meio e final da mídia) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma mídia referente a cada semana. Essas mídias são armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.

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

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

5.1.2.2.6. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, é permanentemente monitorado por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras 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 DOCCLOUD em emergências. 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 emergências.

5.1.3. Energia e Ar-condicionado

5.1.3.1. A infraestrutura do ambiente de certificação da AC DOCCLOUD 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 DOCCLOUD 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 utilizados tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, de telefonia e de dados.

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

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

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

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

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

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

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

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

5.1.4. Exposição à água

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

5.1.5. Prevenção e proteção contra incêndio

5.1.5.1. Todas as instalações da AC DOCCLOUD 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 DOCCLOUD não é permitido fumar ou portar objetos que produzam fogo ou faísca.

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

5.1.5.4. Em caso de incêndio nas instalações da AC DOCCLOUD, 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 DOCCLOUD atende a norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

5.1.7. Destruição de lixo

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

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

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

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

5.2. CONTROLES PROCEDIMENTAIS

5.2.1. Perfis qualificados

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

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

5.2.1.2 A AC DOCCLOUD estabelece 21 (vinte e um) perfis distintos, agrupados em 6 (seis) equipes, para manter o princípio de segregação de tarefas na sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. As responsabilidades e níveis de acesso estão descritas em documentação interna. As equipes e os perfis estabelecidos são:

a) GERÊNCIA
a.1) GERENTE DA AC

b) COMPLIANCE
b.1) COORDENADOR DE COMPLIANCE
b.2) OPERADOR DE COMPLIANCE

c) SISTEMAS
c.1) COORDENADOR DE SISTEMAS
c.2) ADMINISTRADOR DE SISTEMAS
c.3) DESENVOLVEDOR DE SISTEMAS

d) INFRAESTRUTURA
d.1) COORDENADOR DE INFRAESTRUTURA
d.2) ADMINISTRADOR DE DOMÍNIO
d.3) ADMINISTRADOR DE INFRAESTRUTURA
d.4) ADMINISTRADOR DE REDE
d.5) ADMINISTRADOR DE BANCO DE DADOS
d.6) ADMINISTRADOR DE BACKUP
d.7) OPERADOR DE INFRAESTRUTURA

e) OPERACIONAL
e.1) COORDENADOR OPERACIONAL
e.2) DETENTOR DE CHAVES DE HSM
e.3) OPERADOR DE ADMINISTRAÇÃO DE PESSOAS
e.4) OPERADOR DE DESENVOLVIMENTO HUMANO E ORGANIZACIONAL
e.5) OPERADOR DE SERVIÇOS
e.6) VIGILANTE

f) SEGURANÇA DA INFORMAÇÃO
f.1) COORDENADOR DE SEGURANÇA DA INFORMAÇÃO
f.2) AUDITOR INTERNO

5.2.1.3. Todos os operadores do sistema de certificação da AC DOCCLOUD 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.

5.2.1.3.1 Item não aplicável.

5.2.1.4. A AC DOCCLOUD possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos seus funcionários. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o funcionário devolve à AC DOCCLOUD 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 DOCCLOUD, 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 DOCCLOUD requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC DOCCLOUD podem 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 DOCCLOUD passam por um processo rigoroso de seleção. Todo funcionário da AC DOCCLOUD tem sua identidade e perfil verificados antes de:

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

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

a) são diretamente atribuídos a um único operador (funcionário da AC DOCCLOUD 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 DOCCLOUD implementa um padrão de utilização de "senhas fortes", definido em conformidade com a Política de Segurança da AC e DOCCLOUD POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], juntamente com procedimentos de validação dessas senhas.

5.2.4 Funções que requerem separação de deveres

A AC DOCCLOUD impõe a separação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3. CONTROLES DE PESSOAL

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC DOCCLOUD e pela AR DOCCLOUD 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 DOCCLOUD e da AR DOCCLOUD, 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 DOCCLOUD;
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 DOCCLOUD envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados são admitidos conforme o estabelecido na Política de Segurança da AC DOCCLOUD 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 DOCCLOUD, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, são submetidos 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.

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

5.3.3. Requisitos de treinamento

Todo o pessoal da AC DOCCLOUD 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 DOCCLOUD e da AR vinculada;
b) sistema de certificação em uso na AC DOCCLOUD;
c) procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e da validade dos documentos apresentados, na forma dos itens 3.2.2 e 3.2.3; e
e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC DOCCLOUD e da Autoridade de Registro vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC DOCCLOUD e no sistema das ARs.

5.3.5. Frequência e sequência de rodízios de cargos

A AC DOCCLOUD não programa rodízio de cargos, de acordo com os propósitos estabelecidos no item 5.2.1 desta DPC para a definição de perfis qualificados.

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 DOCCLOUD 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 DOCCLOUD 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 DOCCLOUD e da ICP-Brasil

5.3.7. Requisitos para contratação de pessoal

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

5.3.8. Documentação fornecida ao pessoal

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

a) a DPC da AC DOCCLOUD;
b) Item não aplicável;
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 DOCCLOUD.

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

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

5.4.1. Tipos de Evento Registrados

5.4.1.1. A AC DOCCLOUD 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 DOCCLOUD;
c) mudanças na configuração da AC DOCCLOUD 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 DOCCLOUD 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.

5.4.1.1.1 Item não aplicável.

5.4.1.2. A AC DOCCLOUD 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.

5.4.1.3. A AC DOCCLOUD não registra outras informações

5.4.1.4. 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.

5.4.1.5. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC DOCCLOUD é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil [8].

5.4.1.6. A AC DOCCLOUD registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são 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; e
d) a assinatura digital do executante.

5.4.1.6.1 Item não aplicável.

5.4.1.7 A AC DOCCLOUD 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.

5.4.2. Frequência de auditoria de registros (logs)

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

5.4.3. Período de Retenção para registros (logs) de Auditoria

A AC DOCCLOUD 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 5.5.

5.4.4 Proteção de registros de auditoria

5.4.4.1. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção através das funcionalidades nativas dos sistemas operacionais. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, através de permissões dadas pelo administrador do sistema de acordo com a função dos usuários ou aplicações e orientação do departamento de segurança. O próprio sistema operacional também registra os acessos aos arquivos onde estão armazenados os registros de auditoria.

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

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

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

5.4.5.1. Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC DOCCLOUD, protegido com o mesmo tipo de proteção utilizada no arquivo principal.

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

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

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

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

5.4.7 Notificação de agentes causadores de eventos

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

5.4.8 Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a AC DOCCLOUD. 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 DOCCLOUD, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

5.5. ARQUIVAMENTO DE REGISTROS

5.5.1. Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC DOCCLOUD:

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 DOCCLOUD;
g) Informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

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

a) as LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
b) as cópias dos documentos de identificação apresentados no momento da solicitação e da revogação de certificados e os termos de titularidade e responsabilidade serão retidos, no mínimo, por 7 (sete) anos a contar da data de expiração ou revogação do certificado; e
c) as demais informações, inclusive registros de auditoria são retidas por, no mínimo, 7 (sete) anos.

5.5.3 Proteção de arquivo

A AC DOCCLOUD estabelece que todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis como tal classificação, conforme a Política de Segurança da AC DOCCLOUD e POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.5.4 Procedimentos de cópia de arquivo

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

5.5.4.2. As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.
5.5.4.3. A AC DOCCLOUD verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5 Requisitos para datação de registros

5.5.5.1. Os servidores estão sincronizados com a hora Greenwich Mean Time (GMT). Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT no formato DD/MM/AAAA HH:MM:SS, inclusive os certificados emitidos por esses equipamentos. No caso dos registros feitos manualmente e formulários de requisição de certificados, estes contêm a Hora Oficial do Brasil.

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

Todos os sistemas de coleta de dados de arquivo utilizados pela AC DOCCLOUD em seus procedimentos operacionais são automatizados, manuais e internos.

5.5.7. Procedimentos para obter e verificar informação de arquivo

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

5.6. TROCA DE CHAVE

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

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

5.7. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

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

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

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

5.7.1.2 Os procedimentos descritos no Plano de Continuidade do Negócio (PCN) da AR DOCCLOUD contemplam a recuperação, total ou parcial das atividades das ARs, contendo, no mínimo as seguintes informações:

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

5.7.2. Recursos computacionais, software ou dados corrompidos.

Os procedimentos de recuperação utilizados pela AC DOCCLOUD, quando recursos computacionais, softwares ou dados estiverem corrompidos ou houver suspeita de corrupção, incluem, mas não se limitam a somente estes:

I. A identificação da crise;
II. Acionamento dos principais gestores;
III. Ativação das equipes;
IV. Contenção da crise;
V. Estimativa do alargamento da crise;
VI. Declaração do início das atividades de ativação da situação de recuperação;
VII. Notificação da crise;
VIII. Registro da crise; e
IX. Crítica para melhoria.

5.7.2.1 Nas circunstâncias de crise relacionadas aos recursos computacionais, softwares e dados corrompidos ou quando houver suspeita de corrupção desses components, após a identificação da crise ou confirmação da suspeita de corrupção, são comunicados os gestores de certificação digital, que acionam as equipes, de forma a identificar o grau de corrupção.

5.7.2.3 Os métodos de recuperação dos recursos computacionais, softwares e dados corrompidos envolvem: identificação da necessidade de recurso computacional alternativo e, em caso de necessidade, disponibilização de outro recurso computacional equivalente, instalação dos softwares necessários e recuperação dos dados através do arquivo de backup, conforme detalhado em documentação interna.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado de entidade é revogado

Em caso de revogação do certificado da AC DOCCLOUD a Diretoria, juntamente com a Supervisão de PKI da AC DOCCLOUD, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados e a AC DOCCLOUD emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

5.7.3.2 Chave de entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC DOCCLOUD, o fato é imediatamente comunicado a Diretoria que, juntamente com a Supervisão de PKI da AC DOCCLOUD, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

a) Todos os certificados afetados serão revogados e as partes serão notificadas.
b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC DOCCLOUD estiver encerrando suas atividades.

5.7.4 Capacidade de continuidade de negócio após desastre

Em caso de desastre natural ou de outra natureza, depois da identificação da crise são comunicados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de exposição e comprometimento do ambiente. Na confirmação do desastre e constatado impossibilidade de operação no site principal, as atividades são transferidas para o site de contingência/recuperação de desastre.

5.8. EXTINÇÃO DA AC DOCCLOUD

Em caso de extinção da AC DOCCLOUD ou PSS serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

Os procedimentos incluem, mas não estão limitados à divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, aplicativos dedicados à certificação digital, guarda de bases de dados e registros observará os mesmos requisitos de segurança exigidos pela AC DOCCLOUD.

6. CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1. Geração do Par de Chaves

6.1.1.1 O par de chaves criptográficos da AC DOCCLOUD é gerado pela própria AC DOCCLOUD em módulo criptográfico de hardware, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil. A geração do par de chaves da AC DOCCLOUD é feita pelo titular do certificado correspondente, em processo verificável na presença de pessoas de confiança e treinados para a função.

6.1.1.2 O par de chaves criptográficas de uma AC de nível imediatamente subsequente ao da AC DOCCLOUD é gerado pela própria AC, por intermédio de seu representante legal ou procurador, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil, em cerimônias específicas realizada no PSS da AC DOCCLOUD, na presença de funcionários designados para a função. As cerimônias obedecem a procedimentos formalizados, controlados e passíveis de auditoria.

6.1.1.3 Item não aplicável.

6.1.1.4 O processo de geração do par de chaves da AC DOCCLOUD e de Autoridades Certificadoras subsequentes é feito por hardware.
6.1.1.5 Item não aplicável.

6.1.1.6 O módulo criptográfico utilizado para armazenamento da chave privada da AC DOCCLOUD e ACs subsequentes possui certificação INMETRO, conforme indicado em em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.2 Entrega da chave privada à entidade

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

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1 Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC DOCCLOUD fará uso do padrão PKCS#10.
6.1.3.2 Essa entrega é feita por representante legalmente constituído da AC, em cerimônia específica, em data e hora previamente estabelecidas pela AC DOCCLOUD. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

6.1.4. Entrega de chave pública da AC às terceiras partes

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

a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil;
b) Diretório;
c) na página web: www.doccloud.com.br/repositorios/acdoccloud;
d) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1 Item não aplicável.

6.1.5.2 O tamanho mínimo das chaves criptográficas associadas aos certificados da AC DOCCLOUD e ACs subsequentes é de RSA 4096 bits, conforme em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

6.1.6.1. Os parâmetros de geração de chaves assimétricas dos certificados de AC adotam, no mínimo, o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

6.1.7.1. As chaves criptográficas dos certificados de AC SUBSEQUENTE emitidos pela AC DOCCLOUD poderão ser utilizadas apenas para assinatura dos certificados por elas emitidos e de suas LCRs.

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

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

A AC DOCCLOUD implementa uma combinação de controles físicos (item 5.1.2), lógicos e procedimentais (item 5.2), de forma a garantir a segurança de suas chaves privadas. As chaves privadas da AC DOCCLOUD 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. Os titulares de certificados emitidos pela AC DOCCLOUD, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção

de perda, divulgação, modificação ou uso desautorizado das suas chaves privadas.

6.2.1. Padrões para módulo criptográfico

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

6.2.1.2 O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas possui certificação INMETRO, conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2. Controle "n de m" para chave privada

6.2.2.1 Para a utilização das suas chaves privadas, a AC DOCCLOUD define forma de controle múltiplo, do tipo "n" pessoas de um grupo de "m".

6.2.2.2 A AC DOCCLOUD estabelece como exigência de controle múltiplo para a utilização das suas chaves privadas: 2 (dois) de um grupo de 8 (oito) pessoas com perfis qualificados da AC DOCCLOUD, detentores de partição da chave de ativação do equipamento criptográfico para utilização das suas chaves privadas.

6.2.3. Custódia (escrow) de chave privada

A AC DOCCLOUD não implementa tal prática.

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 DOCCLOUD 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 DOCCLOUD não mantém cópia de segurança das chaves privadas das ACs de nível imediatamente subsequentes ao seu.

6.2.4.4. A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+, ou outros definidos conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC DOCCLOUD não arquiva cópias de chaves privadas de titulares de certificados.

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

6.2.6. Inserção de chave privada em módulo criptográfico

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

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

6.2.8.1. A ativação das chaves privadas das AC DOCCLOUD é coordenada pelo setor de Compliance, onde 2 (dois) de um grupo de 8 (oito) pessoas com perfis qualificados da AC DOCCLOUD, detentores de partição da chave de ativação do equipamento criptográfico, utilizam tais componentes, juntamente com suas senhas em cerimônia específica. Essas pessoas são identificadas pelo crachá funcional emitido pela AC DOCCLOUD contendo fotografia, nome, e departamento do funcionário.

6.2.8.2 A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

6.2.9. Método de desativação de chave privada

6.2.9.1 A chave privada da AC DOCCLOUD, está instalada no ambiente de nível 4, onde só é permitido o acesso em duplas devidamente autorizadas pelo sistema de controle de acesso da AC DOCCLOUD. Somente as pessoas qualificadas, após a sua devida identificação e autorização feita através de utilização de senhas, têm acesso ao sistema de certificação de produção, onde são executados os comandos de desativação da chave privada em cerimônia específica. Essas pessoas são identificadas pelo crachá funcional emitido pela AC DOCCLOUD contendo fotografia, nome, e departamento do funcionário.

6.2.9.2 A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

6.2.10. Método de destruição de chave privada

6.2.10.1 Para a destruição das chaves privadas da AC DOCCLOUD exige-se 2 (dois) de um grupo de 8 (oito) pessoas com perfis qualificados. A confirmação da identidade dessas pessoas é feita através de crachás e senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. As mídias de armazenamento das chaves privadas originais e suas cópias de segurança são reinicializadas de forma a não restarem nelas informações sensíveis, conforme cerimônia específica realizada no ambiente de nível 4 (quatro).

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. Arquivamento de chave pública

A chave pública da própria AC DOCCLOUD, e dos certificados por ela emitidos, bem como as LCR emitidas, serão armazenados pela AC DOCCLOUD, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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

6.3.2.1. As chaves privadas da AC DOCCLOUD e de ACs subsequentes emitidas por ela são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo período determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Item não aplicável.

6.3.2.3. Item não aplicável.

6.3.2.4. A validade admitida para certificados de AC Subsequente é limitada à validade do certificado da AC DOCCLOUD, desde que mantido o padrão de algoritmo para a geração de chaves assimétricas implementado.

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 DOCCLOUD são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em hardware (token ou cartão criptográfico).

6.4.1.2. Item não aplicável.

6.4.2. Proteção dos dados de ativação.

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

6.4.3. Outros aspectos dos dados de ativação

Item não aplicável.

6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A AC DOCCLOUD garante que a geração de seu par de chaves é realizada em ambiente offline, para impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos gerais de segurança computacional dos equipamentos utilizados para a geração dos pares de chaves criptográficas das ACs titulares de certificados emitidos pela AC DOCCLOUD devem ser os mesmos descritos no item abaixo para os computadores servidores da AC DOCCLOUD.

6.5.1.3. Os computadores servidores, utilizados pela AC DOCCLOUD, 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 DOCCLOUD;
b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC DOCCLOUD;
c) acesso restrito aos bancos de dados da AC DOCCLOUD;
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 DOCCLOUD;
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 DOCCLOUD ou da AC subordinada, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC DOCCLOUD ou AC subsequente. Todos esses eventos são registrados para fins de auditoria.

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

6.5.2. Classificação da segurança computacional

A segurança computacional da AC DOCCLOUD segue as recomendações Common Criteria.

6.5.3. Controle de segurança para as Autoridades de Registro

6.5.3.1 A AC DOCCLOUD implementa requisitos de segurança computacional nas estações de trabalho e nos computadores portáteis utilizados pela AR DOCCLOUD para os processos de validação e aprovação de certificados.

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

a) controle de acesso lógico ao sistema operacional;
b) exigência de uso de senhas fortes;
c) diretivas de senha e de bloqueio de conta;
d) logs de auditoria do sistema operacional ativados, registrando:
    i. iniciação e desligamento do sistema;
    ii. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
    iii. mudanças na configuração da estação;
    iv. tentativas de acesso (login) e de saída do sistema (logoff);
    v. tentativas não autorizadas de acesso aos arquivos de sistema;
    vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves
e) antivírus, antitrojan e antispyware, instalados, atualizados e habilitados;
f) firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo;
g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
h) sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
i) utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
j) impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
k) utilização de data e hora de Fonte Confiável do Tempo (FCT).

6.5.3.3. Item não aplicável.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1. Controles de desenvolvimento de sistemas

6.6.1.1 A AC DOCCLOUD utiliza metodologias ágeis no desenvolvimento dos sistemas. São realizadas as fases de análise de requisitos, codificação, testes e homologação (pré-produção) para cada interação do sistema. Como suporte a esse modelo, a AC DOCCLOUD utiliza uma gerência de configuração, gerência de mudanças, testes formais e outros processos. As estações de trabalho e servidores utilizados pelos desenvolvedores dos sistemas da AC DOCCLOUD possuem controles de segurança implementados a fim de garantir um ambiente segregado, mantendo o controle e integridade do processo de desenvolvimento.

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

6.6.2. Controle de gerenciamento de segurança

6.6.2.1 A AC DOCCLOUD e AR DOCCLOUD utilizam ferramentas específicas para verificação da configuração de segurança dos seus sistemas semanalmente. Os dados coletados durante a verificação periódica são comparados com as configurações aprovadas. Caso haja divergência, são tomadas medidas adequadas para a recuperação da situação, levando-se em consideração a natureza do problema e a análise do fato gerador, para evitar a sua recorrência.

6.6.2.2 A AC DOCCLOUD utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do seu sistema de certificação.

6.6.3. Controles de segurança de ciclo de vida

Item não aplicável.

6.6.4. Controles na Geração de LCR

Antes de publicadas todas as LCR geradas pela AC DOCCLOUD 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 A AC DOCCLOUD implementa os seguintes controles de segurança de rede:

a) Firewall de:
- a.1) rede;
- a.2) host; e
- a.3) aplicação.

b) Segregação de tráfego utilizando VLANs;
c) Sistema de detecção e prevenção de intrusão de:
- c.1) rede; e
- c.2) host.

d) Antivírus;

e) Sandbox;

f) Filtragem web; e

g) Monitoramento 24x7.

6.7.1.2 Nos servidores do sistema de certificação da AC DOCCLOUD, somente os serviços estritamente necessários são habilitados.

6.7.1.3 Todos os servidores e elementos de infraestrutura e proteção de rede, localizados no segmento de rede que hospeda o sistema de certificação da AC DOCCLOUD, estão localizados e operam em ambiente de nível 4 (quatro).

6.7.1.4 As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as suas eventuais correções, disponibilizadas pelos respectivos fabricantes, são implantadas 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 A AC DOCCLOUD utiliza firewalls dedicados que promovem o isolamento dos servidores com acesso externo em uma DMZ, separando-os dos servidores que possuem acesso exclusivamente interno.

6.7.2.2 O firewall utilizado pela AC DOCCOUD o registro dos eventos em logs, além de implementar uma gerência de configuração

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

6.7.4.1 As tentativas de acesso não autorizado são registradas para posterior análise. Esses registros são analisados diariamente e todas as ações tomadas em decorrência dessa análise são documentadas.

6.8. CARIMBO DE TEMPO

Item não aplicável.

7. PERFIS DE CERTIFICADO E LCR

7.1. Perfil do Certificado

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

7.1.1. Número de versão

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

7.1.2. Extensões de certificado

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

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

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

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

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

d.1) o campo policyIdentifier contém: os OID das PCs que a AC titular do certificado implementa

d.2) o campo *policyQualifiers* contém o endereço URL da *página web onde se obtém a DPC da AC DOCCLOUD:* http://repositorio.acdoccloud.com.br/ac-doccloud/dpc-acdoccloud.pdf

e) *basicConstraints*, crítica: contém o campo CA=True; e

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

f.1 http://repositorio.acdoccloud.com.br/ac-doccloud/lcr-ac-doccloud.crl

f.2 http://repositorio2.acdoccloud.com.br/ac-doccloud/lcr-ac-doccloud.crl

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC DOCCLOUD são assinados com a suíte de assinatura sha512WithRSAEncryption, conforme definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.4. Formatos de nome

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

C=BR
O= ICP-Brasil
OU= AC DOCCLOUD
CN= Nome da AC TITULAR

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

7.1.5. Restrições de nome

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

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

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

7.1.6. OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC DOCCLOUD após conclusão do processo de seu credenciamento, é **2.16.76.1.1.81**.

7.1.7. Uso da extensão "Policy Constraints"

Item não aplicável.

7.1.8. Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC DOCCLOUD http://repositorio.acdoccloud.com.br/ac-doccloud/dpc-acdoccloud.pdf.

7.1.9. Semântica de processamento para extensões críticas de PC.

Item não aplicável.

7.2. PERFIL DE LCR

7.2.1. Número (s) de versão

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

7.2.2. Extensões de LCR e de suas entradas

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

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

a) "Authority Key Identifier", não crítica, contém o hash SHA-1 da chave pública da AC DOCCLOUD que assina a LCR.

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

7.3. PERFIL DE OCSP

Item não aplicável.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. FREQUÊNCIA E CIRCUNSTÂNCIA DAS AVALIAÇÕES

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

8.2. IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

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

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

8.3. RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

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

8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO

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

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

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

8.5. AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

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

De acordo com os procedimentos relacionados nos documentos acima mencionados, a AC DOCCLOUD cumprirá os prazos estipulados em relatórios de auditorias, as recomendações para corrigir as não-conformidades, com a legislação o com as políticas, normas práticas e regras estabelecidas.

8.6. COMUNICAÇÃO DOS RESULTADOS

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

De acordo com os procedimentos relacionados nos documentos acima mencionados, a AC DOCCLOUD assim que cumpridas todas as exigências apontadas, comunicará à AC RAIZ anexando cópia de correspondências trocadas, evidências da inconformidade e das ações adotadas até o momento para mitigação do(s) risco(s) envolvido(s).

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. TARIFAS

9.1.1. Tarifas de emissão e renovação de certificados

Variável conforme definição interna Comercial.

9.1.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

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

9.1.4. Tarifas para outros serviços

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

9.1.5. Política de reembolso

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

9.2. RESPONSABILIDADE FINANCEIRA

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

9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2 Outros ativos

Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para AC SUBSEQUENTE

A AC DOCCLOUD implementa uma política que contém informações sobre a utilização correta da garantia oferecida sobre os seus certificados digitais e está de acordo com a legislação vigente, especialmente, o Código de Defesa do Consumidor (CDC). A Política de Garantia está disponível no site da AC, através do link: www.doccloud.com.br/repositorios/acdoccloud

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 Escopo de informações confidenciais

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

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

9.3.2 Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas compreendem:

a) LCR de certificados emitidos pela AC DOCCLOUD;
b) informações corporativas ou pessoais que façam parte do certificados ou em diretórios públicos;
c) esta DPC;
d) versões públicas da Política de Segurança;
e) resultados finais de auditorias; e
f) Termo de Titularidade ou solicitação de emissão do certificado para AC SUBSEQUENTE.

A AC DOCCLOUD trata 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 DOCCLOUD 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 sua sem quaisquer restrições para tal;
c) sejam requisitados por determinação judicial ou governamental, desde que a AC DOCCLOUD comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

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

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

9.3.2.2 Os seguintes documentos da AC DOCCLOUD também são considerados documentos não confidenciais:

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

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

9.3.3 Responsabilidade em proteger a informação confidencial

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

9.3.3.2. A chave privada de assinatura digital da AC DOCCLOUD será gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC será de sua inteira responsabilidade.

9.3.3.3. Item não aplicável.

9.3.3.4. Item não aplicável.

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1 Plano de privacidade

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

9.4.2 Tratamento de informação como privadas

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

9.4.3 Informações não consideradas privadas

Informações sobre revogação de certificados de AC de nível imediatamente subsequente ao da AC DOCCLOUD são fornecidas na LCR da propria AC DOCCLOUD.

9.4.4 Responsabilidade para proteger a informação privadas

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

9.4.5 Aviso e consentimento para usar informações privadas

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

A AC SUBSEQUENTE terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

Autorizações formais podem ser apresentadas de duas formas:

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

9.4.6 Divulgação em processo judicial ou administrativo

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC DOCCLOUD será fornecido a qualquer pessoa, salvo se autorizado pela AC SUBSEQUENTE.

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

9.4.7 Outras circunstâncias de divulgação de informação

Item não aplicável.

9.4.8 Informações a terceiros

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

9.5 DIREITOS DE PROPRIEDADE INTELECTUAL

De acordo com a legislação vigente

9.6 DECLARAÇÕES E GARANTIAS

9.6.1 Declarações e Garantias da AC DOCCOUD

A AC DOCCLOUD declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

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

9.6.1.2 Precisão da informação

A AC DOCCLOUD implementa procedimentos para verificar a precisão da informação nos certificados, contidas

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

9.6.1.3 Identificação do requerente

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

9.6.1.4 Consentimento dos titulares

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

9.6.1.5 Serviços

A AC DOCCLOUD mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios, das ACs subsequentes e LCRs/OCSP.

9.6.1.6 Revogação

A AC DOCCLOUD irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos documentos Baseline Requirements, EV SSL Guidelines e/ou EV CS Guidelines.

9.6.1.7 Existência legal

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

9.6.2 Declarações e Garantias da AR DOCCLOUD

Em acordo com item 4 desta DPC.

9.6.3 Declarações e garantias do titular

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

9.6.3.2 A AC DOCCLOUD informará à AC Raiz qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

9.6.4 Declarações e garantias das terceiras partes

9.6.4.1 A AC SUBSEQUENTE deve:

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

9.6.4.2 O certificado da AC DOCCLOUD ou um certificado de AC de nível imediatamente subsequente ao da AC DOCCLOUD é considerado válido quando:

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

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

9.6.5 Representações e garantias de outros participantes

Item não aplicável

9.7 ISENÇÃO DE GARANTIAS

Item não aplicável

9.8 LIMITAÇÕES DE RESPONSABILIDADE

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

9.9 INDENIZAÇÕES

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

9.10 PRAZO E RESCISÃO

9.10.1 Prazo

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

9.10.2 Término

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

9.10.3 Efeito da rescisão e sobrevivência

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

9.11 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM PARTICIPANTES

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

9.12. ALTERAÇÕES

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC DOCCLOUD mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web.

9.12.3. Circunstâncias na qual o OID deve ser alterado

Item não aplicável

9.13. SOLUÇÃO DE CONFLITOS

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

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

9.14. LEI APLICÁVEL

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

9.15. CONFORMIDADE COM A LEI APLICÁVEL

A AC DOCCLOUD está sujeita à Legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em Lei.

9.16. DISPOSIÇÕES DIVERSAS

9.16.1. Acordo completo

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

9.16.2. Cessão

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

9.16.3. Independência de disposições

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

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

De acordo com a legislação vigente.

9.17. OUTRAS PROVISÕES

Item não aplicável.

10. DOCUMENTOS REFERENCIADOS

10.1. 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

	Aprovado pela Resolução nº 25, de 24 de outubro de 2003	
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001	DOC-ICP-02

10.2. 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

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 11.515/NB 1334: Critérios de segurança física relativos ao armazenamento de dados. 2007.

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

RFC 4210, IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), september 2005.

RFC 5280, IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, may 2008.
RFC 6712, IETF - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.